

Issues report for Security Test 2

in 164.90.157.161-withUsernamePassword/Security Test Suite 1/https://164.90.157.161 TestCase

Summary

Started at 2021-04-16 11:51:01

Time taken 00:00:07.634

Total scans performed: 62

Issues found: 12

Scan	Issues Found In Test Steps		Total Issues Found
HTTP Method Fuzzing	GET	12	12

Detailed Info

Issues are grouped by Security scan.

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://164.90.157.161/	
Request	PURGE https://164.90.157.161/ HTTP/1.1	
Test Step	GET	
Modified Parameters	Name	Value
	method	PURGE
Response	Content-type: text/html; charset=utf-8 Content length: 141 Full response:	

	<pre><!DOCTYPE html> <html lang="en"> <head> <meta charset="utf-8"> <title> Error</title> </head> <body> <pre>Cannot PURGE </pre> </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 <code>PURGE</code> should really be allowed for this resource.	
Issue Number	#1	

Scan	HTTP Method Fuzzing					
Severity	WARNING					
Endpoint	https://164.90.157.161/					
Request	COPY https://164.90.157.161/ 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	<div><p>Content-type: text/html; charset=utf-8</p><p>Content length: 140</p><p>Full response:</p><pre><!DOCTYPE html> <html lang="en"> <head> <meta charset="utf-8"> <title> Error</title> </head> <body> <pre>Cannot COPY </pre> </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 <code>COPY</code> should really be allowed for this resource.					
Issue Number	#2					

Scan

Severity

Endpoint

Request

Test Step

Modified Parameters

Response

Alerts

Action Points

Issue Number

HTTP Method Fuzzing

WARNING

https://164.90.157.161/

UNLOCK https://164.90.157.161/ HTTP/1.1

GET

Name	Value
method	UNLOCK

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

Content length: 142

Full response:

<!DOCTYPE html> <html lang="en"> <head> <meta charset="utf-8"> <title>Error</title> </head> <body> <pre>Cannot UNLOCK </pre> </body> </html>

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

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

#3

Scan	HTTP Method Fuzzing	
Severity	WARNING	
Endpoint	https://164.90.157.161/	
Request	LOCK https://164.90.157.161/ 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	Content-type: text/html; charset=utf-8 Content length: 140 Full response: <pre><!DOCTYPE html> <html lang="en"> <head> <meta charset="utf-8"> <title> Error</title> </head> <body> <pre>Cannot LOCK </pre> </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 LOCK should really be allowed for this resource.				
Issue Number	#4				

Scan	HTTP Method Fuzzing				
Severity	WARNING				
Endpoint	https://164.90.157.161/				
Request	PROPFIND https://164.90.157.161/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>method</td><td>PROPFIND</td></tr> </table>	Name	Value	method	PROPFIND
Name	Value				
method	PROPFIND				
Response	Content-type: text/html; charset=utf-8 Content length: 144 Full response: <pre><!DOCTYPE html> <html lang="en"> <head> <meta charset="utf-8"> <title> Error</title> </head> <body> <pre>Cannot PROPFIND </pre> </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 PROPFIND should really be allowed for this resource.				
Issue Number	#5				

Scan	HTTP Method Fuzzing				
Severity	WARNING				
Endpoint	https://164.90.157.161/				
Request	PATCH https://164.90.157.161/ HTTP/1.1				
Test Step	GET				
Modified Parameters	<table> <tr> <th>Name</th><th>Value</th></tr> <tr> <td>method</td><td>PATCH</td></tr> </table>	Name	Value	method	PATCH
Name	Value				
method	PATCH				
Response	Content-type: text/html; charset=utf-8 Content length: 141 Full response: <pre><!DOCTYPE html> <html lang="en"> <head> <meta charset="utf-8"> <title> Error</title> </head> <body> <pre>Cannot PATCH </pre> </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 PATCH should really be allowed for this resource.				
Issue Number	#6				

Scan HTTP Method Fuzzing

Severity WARNING

Endpoint https://164.90.157.161/

Request TRACE https://164.90.157.161/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
method	TRACE

Response

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

Content length: 141

Full response:

```
<!DOCTYPE html> <html lang="en"> <head> <meta charset="utf-8"> <title>
Error</title> </head> <body> <pre>Cannot TRACE </pre> </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 TRACE should really be allowed for this resource.

Issue Number

#7

Scan HTTP Method Fuzzing

Severity WARNING

Endpoint https://164.90.157.161/

Request OPTIONS https://164.90.157.161/ HTTP/1.1

Test Step GET

Modified Parameters

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

#8

Scan HTTP Method Fuzzing

Severity WARNING

Endpoint https://164.90.157.161/

Request HEAD https://164.90.157.161/ HTTP/1.1

Test Step GET

Modified Parameters

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 #9

Scan HTTP Method Fuzzing

Severity WARNING

Endpoint https://164.90.157.161/

Request DELETE https://164.90.157.161/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
method	DELETE

Response

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

Content length: 142

Full response:

```
<!DOCTYPE html> <html lang="en"> <head> <meta charset="utf-8"> <title>
Error</title> </head> <body> <pre>Cannot DELETE /</pre> </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 `DELETE` should really be allowed for this resource.

Issue Number #10

Scan HTTP Method Fuzzing

Severity WARNING

Endpoint https://164.90.157.161/

Request PUT https://164.90.157.161/ HTTP/1.1

Test Step GET

Modified Parameters

Name	Value
method	PUT

Response

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

Content length: 139

Full response:

```
<!DOCTYPE html> <html lang="en"> <head> <meta charset="utf-8"> <title>
Error</title> </head> <body> <pre>Cannot PUT /</pre> </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 #11

Scan HTTP Method Fuzzing

Severity WARNING

Endpoint https://164.90.157.161/

Request POST https://164.90.157.161/ HTTP/1.1

Test Step GET

Modified Parameters	Name	Value
	method	POST
Response	Content-type: text/html; charset=utf-8 Content length: 140 Full response: <!DOCTYPE html> <html lang="en"> <head> <meta charset="utf-8"> <title>Error</title> </head> <body> <pre>Cannot POST </pre> </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 <code>POST</code> should really be allowed for this resource.	
Issue Number	#12	