

Preparazione dell'Ambiente:

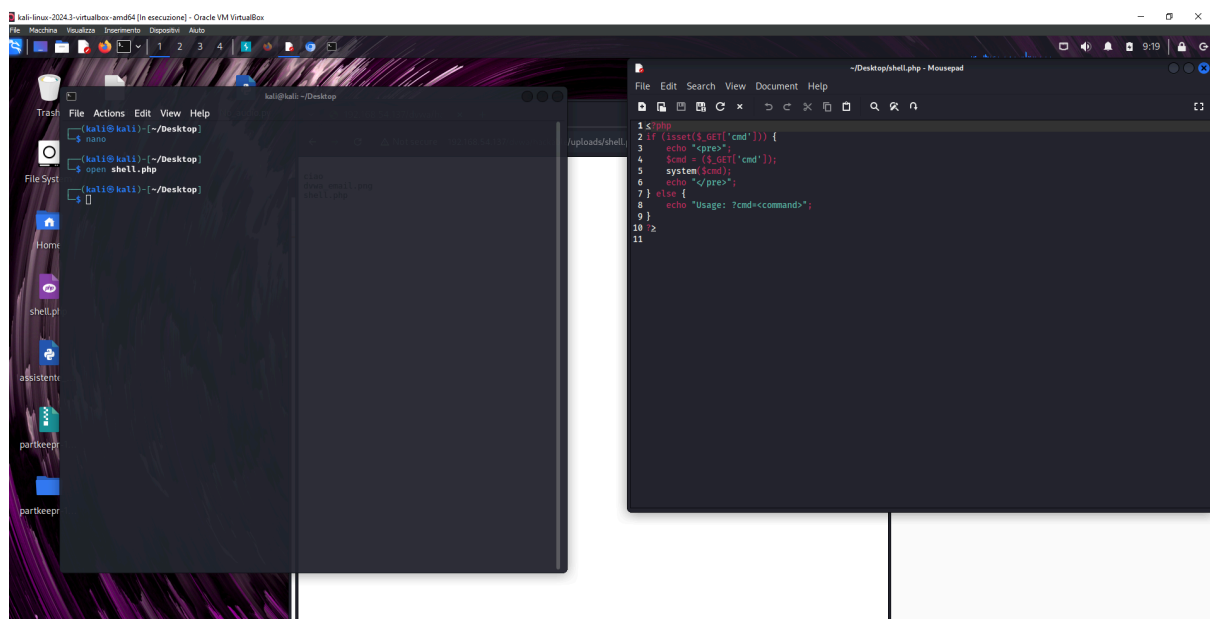
```
lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        RX packets:105 errors:0 dropped:0 overruns:0 frame:0
        TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:25617 (25.0 KB)  TX bytes:25617 (25.0 KB)

msfadmin@metasploitable:~$ ping 192.168.54.136
PING 192.168.54.136 (192.168.54.136) 56(84) bytes of data.
64 bytes from 192.168.54.136: icmp_seq=1 ttl=64 time=0.207 ms
64 bytes from 192.168.54.136: icmp_seq=2 ttl=64 time=0.342 ms
64 bytes from 192.168.54.136: icmp_seq=3 ttl=64 time=0.382 ms
64 bytes from 192.168.54.136: icmp_seq=4 ttl=64 time=0.292 ms
64 bytes from 192.168.54.136: icmp_seq=5 ttl=64 time=0.448 ms
64 bytes from 192.168.54.136: icmp_seq=6 ttl=64 time=0.176 ms
64 bytes from 192.168.54.136: icmp_seq=7 ttl=64 time=0.316 ms
64 bytes from 192.168.54.136: icmp_seq=8 ttl=64 time=0.217 ms
64 bytes from 192.168.54.136: icmp_seq=9 ttl=64 time=0.252 ms
64 bytes from 192.168.54.136: icmp_seq=10 ttl=64 time=0.237 ms
64 bytes from 192.168.54.136: icmp_seq=11 ttl=64 time=0.348 ms
64 bytes from 192.168.54.136: icmp_seq=12 ttl=64 time=0.243 ms
```

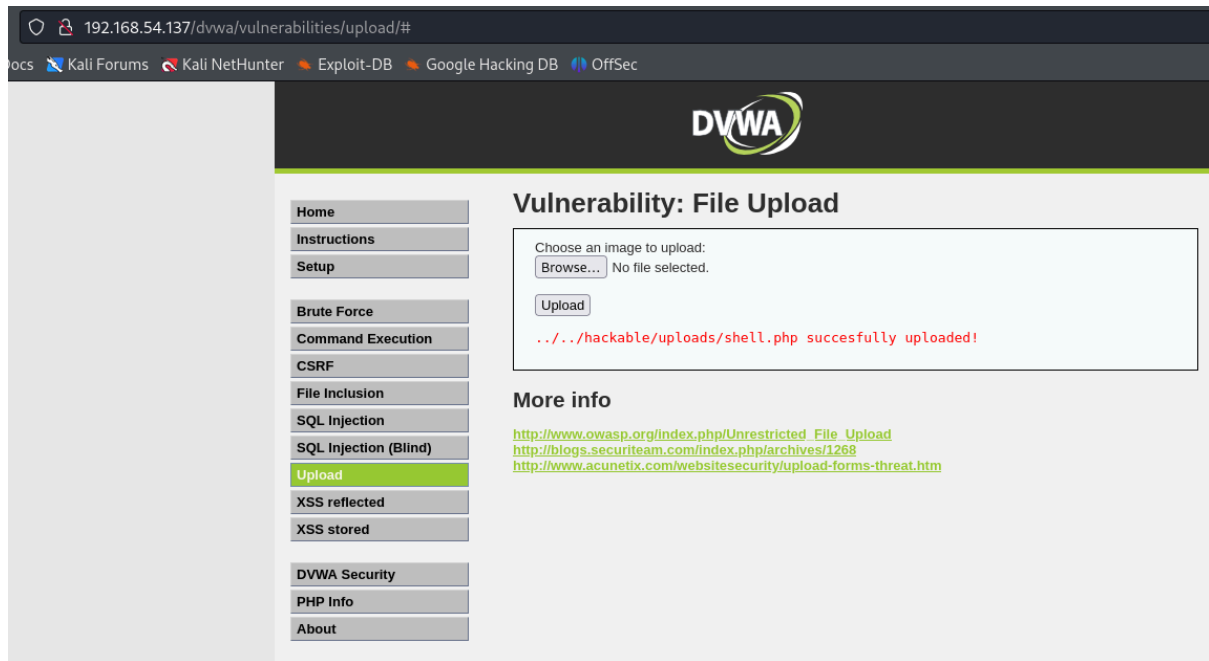
```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ nano
(kali@kali)-[~/Desktop]
$ open shell.php
(kali@kali)-[~/Desktop]
$ ping 192.168.54.137
PING 192.168.54.137 (192.168.54.137) 56(84) bytes of data.
64 bytes from 192.168.54.137: icmp_seq=1 ttl=64 time=0.314 ms
64 bytes from 192.168.54.137: icmp_seq=2 ttl=64 time=0.250 ms
64 bytes from 192.168.54.137: icmp_seq=3 ttl=64 time=0.331 ms
64 bytes from 192.168.54.137: icmp_seq=4 ttl=64 time=0.240 ms
64 bytes from 192.168.54.137: icmp_seq=5 ttl=64 time=0.272 ms
^C
  192.168.54.137 ping statistics ---
  5 packets transmitted, 5 received, 0% packet loss, time 4095ms
 rtt min/avg/max/mdev = 0.240/0.281/0.331/0.035 ms
(kali@kali)-[~/Desktop]
$
```

Verifico che le due macchine comunichino ✓

Caricamento della Shell PHP:

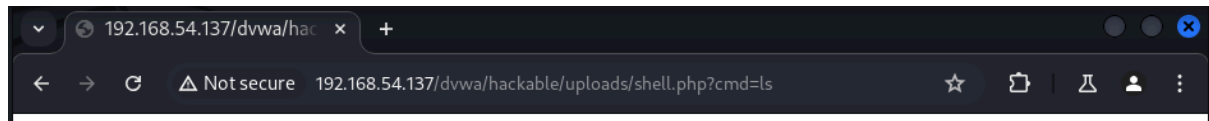


Scriviamo la shell da caricare su DVWA in php e la carichiamo successivamente

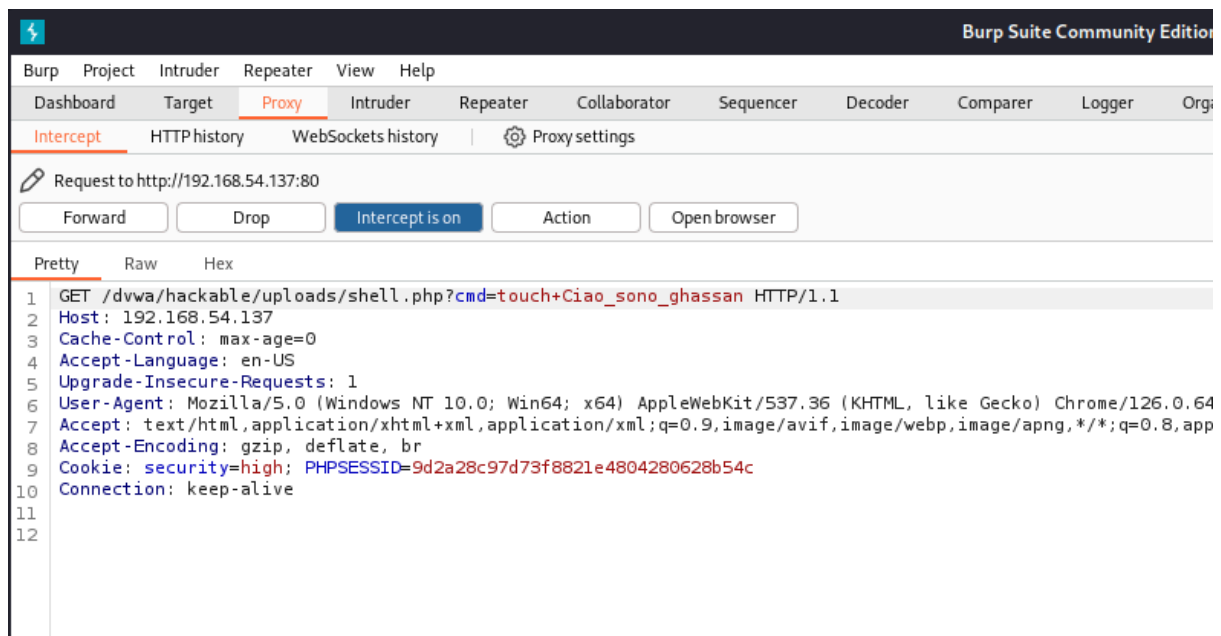


Una volta caricata possiamo procedere su Burpsuite.

Esecuzione della Shell PHP:



una volta sul browser di burpsuite mettiamo l'url per accedere alla shell



Intercettazione e Analisi con BurpSuite:

