S6L1

Obbiettivo: Argomento: Sfruttamento di una vulnerabilità di File Upload sulla DVWA per l'inserimento di una shell in PHP.

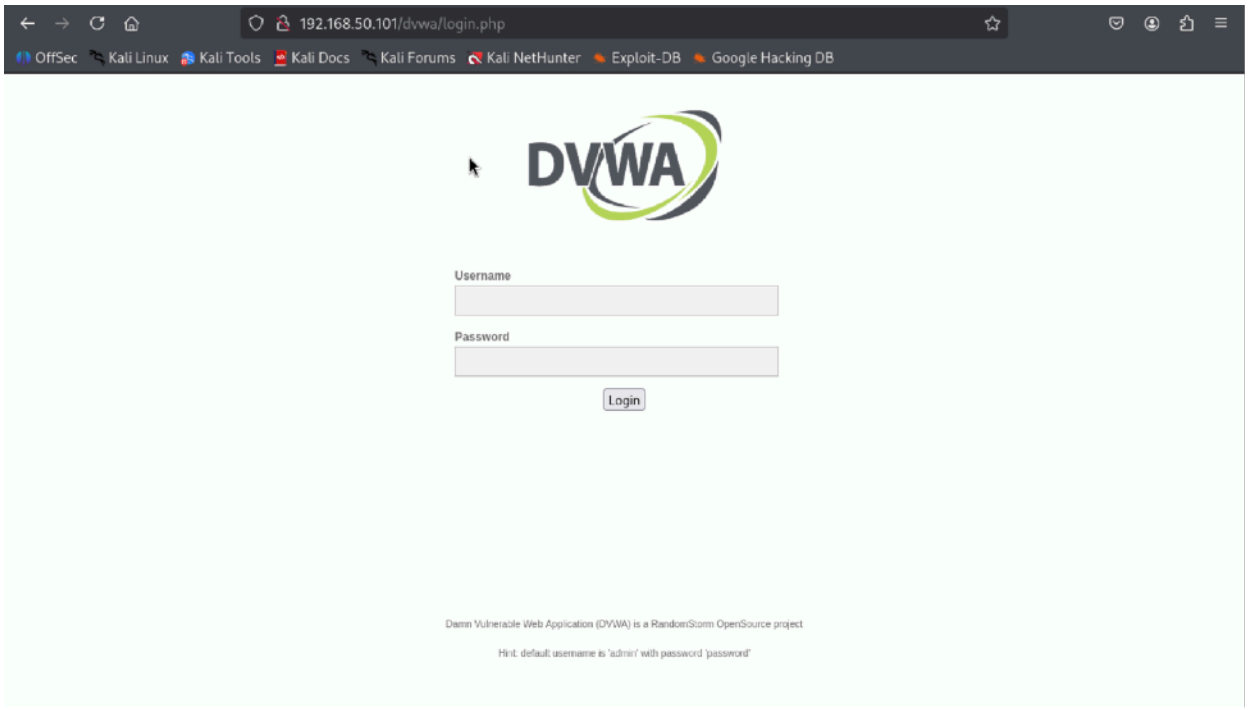
Step1.

Voglio verificare che le due macchine siano configurate in maniera corretta e provo a fare un ping tra le due

```
┌──(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=0.579 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=1.72 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=1.70 ms
^C
── 192.168.50.101 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2014ms
rtt min/avg/max/mdev = 0.579/1.331/1.715/0.532 ms
```

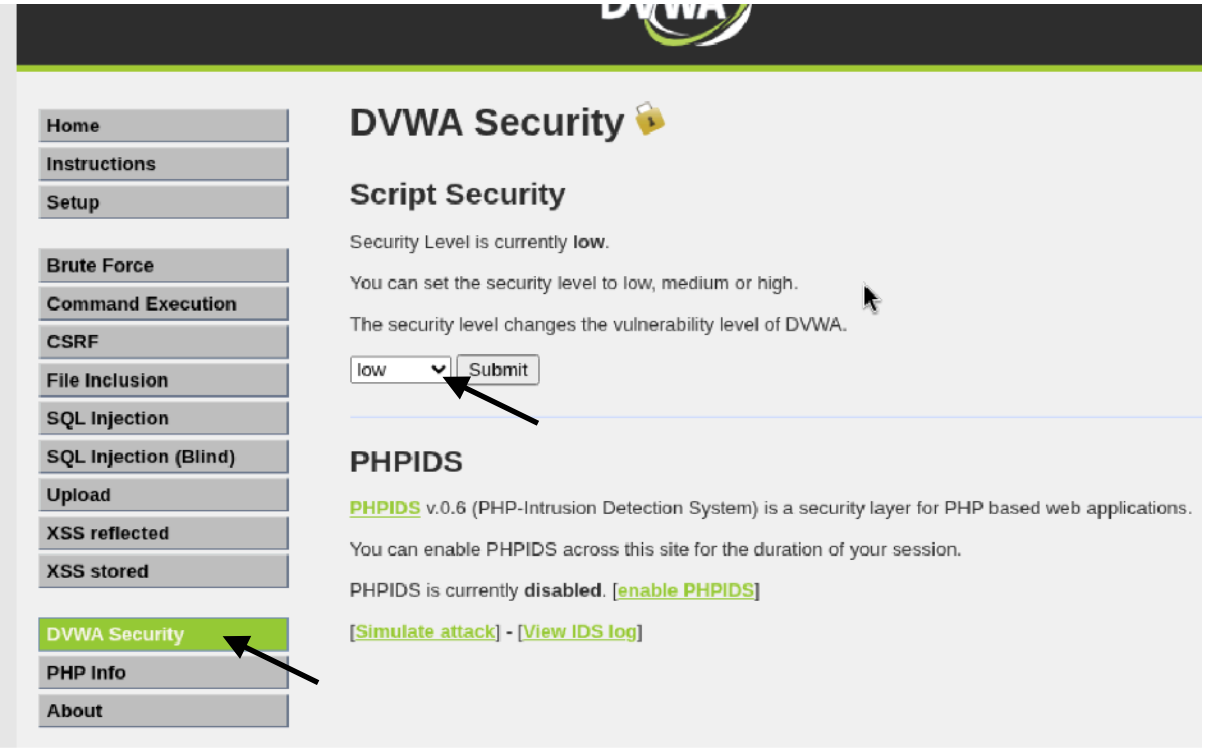
Step2.

Accendo alla DVWA seguendo il processo da BurpSuite



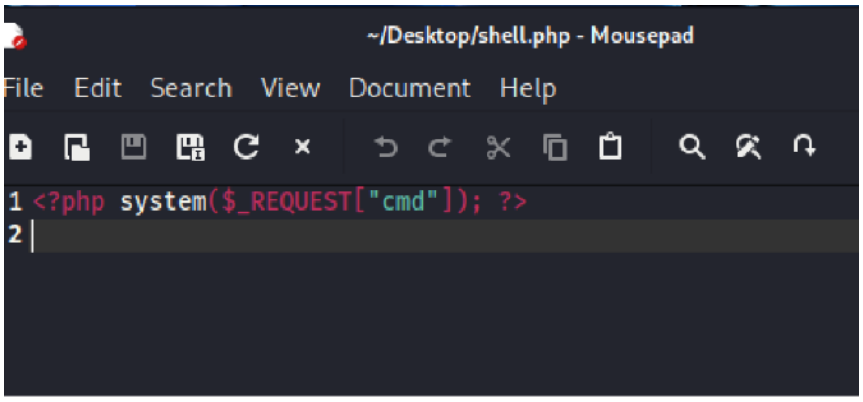
Step3.

Per fare questa prova metterò la sicurezza della DVWA in low quindi vado sulla casella in questione



Step4.

Creo la shell che voglio applicare salvandolo shell.php

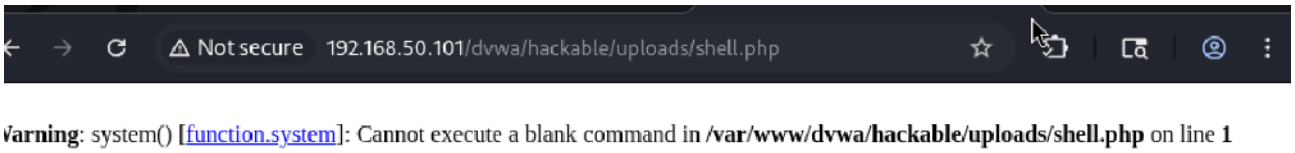


Step5.

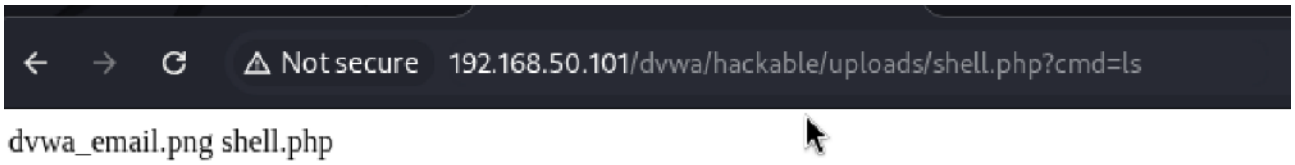
Per installare la shell vado sulla finestra “upload” seleziono il file e faccio Upload

Step6.

Verifico che la shell funzioni andando su “192.168.50.101/dvwa/hackable/uploads/shell.php”



A questo punto mi appare un messaggio che mi dice che il comando non può essere vuoto quindi dopo questa linea inserisco il comando “cmd=ls”

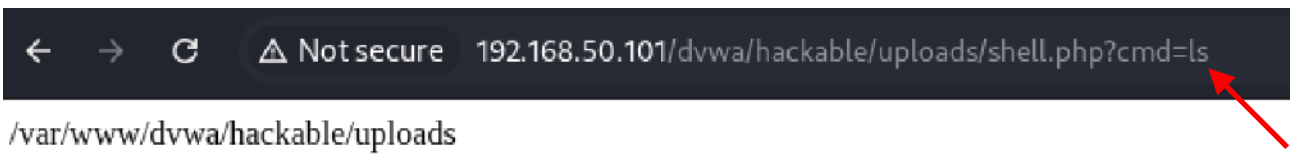


Step7.

Con BurpSuite posso intercettare l’ultima fase e inserire il commando direttamente

Dopo “cmd” provo ad inserire un altro comando ovvero “pwd”

Ora posso vedere che il comando viene eseguito anche senza cambiare l url



Step8.

Ora provo ad inserire un comando che non potrei usare con questa shell come “passwd”

Come si puo vedere non mi da nessun risultato, per usare questo comando dovrei usare una shell più avanzata come ad esempio la r57shell.