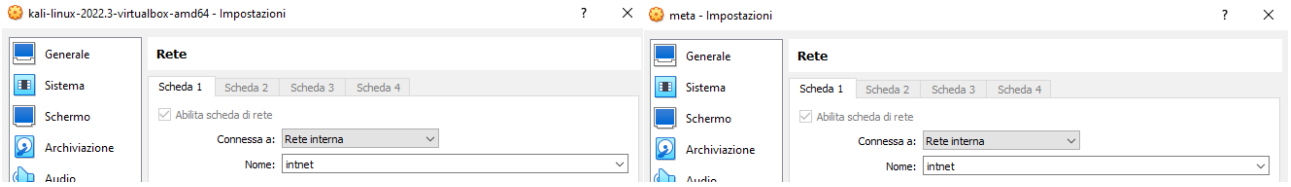
REPORT 28/11/2022 LORENZO SCORBAIOLI

TASK:

Sfruttare un file di upload sulla DVWA per caricare una semplice shell, monitorando gli step con Burpsuite

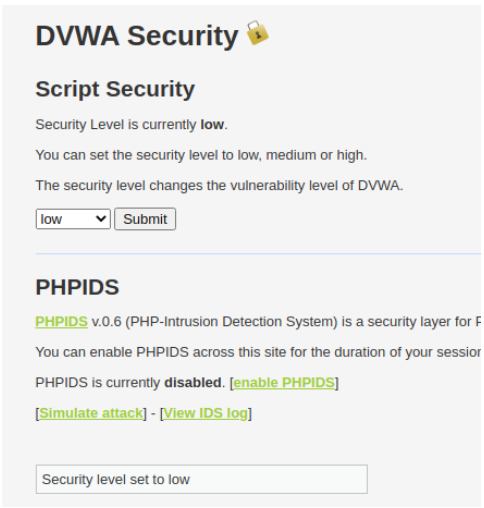
Per prima cosa ho controllato che sia Kali che Metasploitable fossero su rete interna e in comunicazione tra di loro:



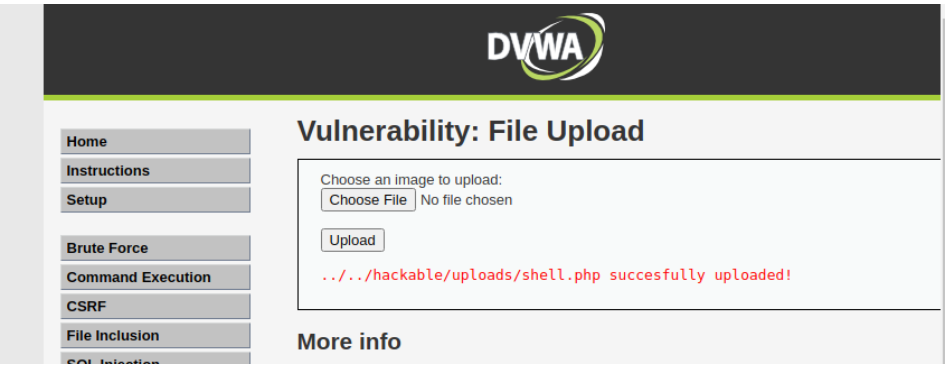

```
┌──(kali㉿kali)-[~]
└─$ ping -c4 192.168.50.111
PING 192.168.50.111 (192.168.50.111) 56(84) bytes of data.
64 bytes from 192.168.50.111: icmp_seq=1 ttl=64 time=0.590 ms
64 bytes from 192.168.50.111: icmp_seq=2 ttl=64 time=0.471 ms
64 bytes from 192.168.50.111: icmp_seq=3 ttl=64 time=0.483 ms
64 bytes from 192.168.50.111: icmp_seq=4 ttl=64 time=0.488 ms

── 192.168.50.111 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3072ms
rtt min/avg/max/mdev = 0.471/0.508/0.590/0.047 ms
```

A questo punto sono andato a creare una semplice webshell in php:

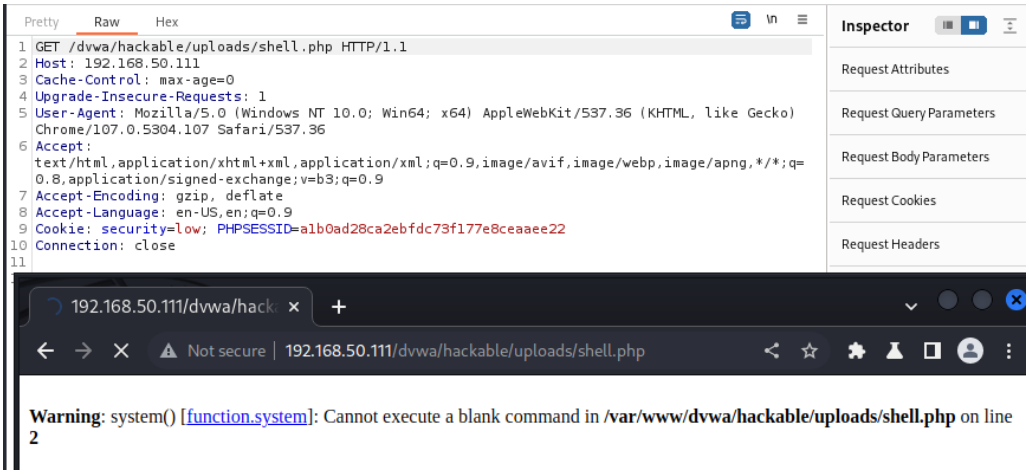
Dopo ciò sono andato a settare il livello di sicurezza di DVWA su low:



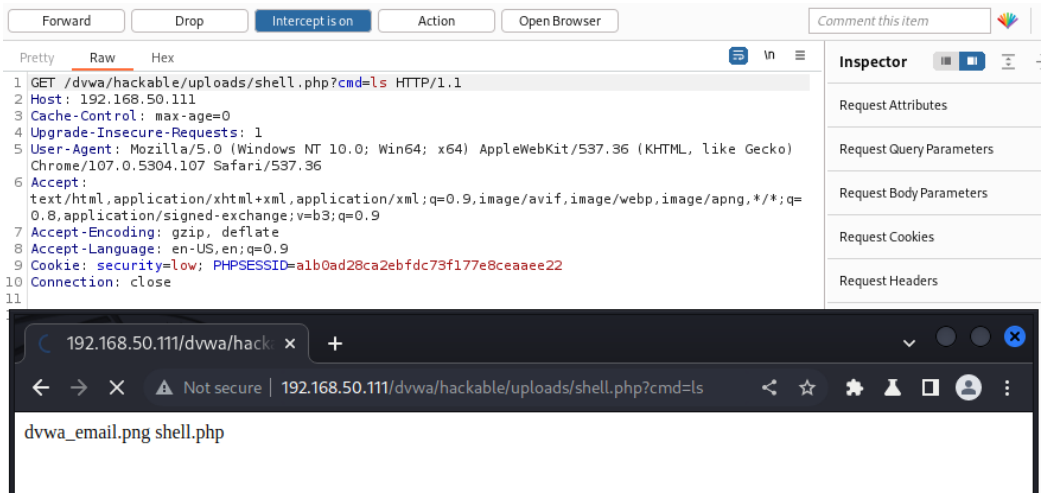
E ho poi caricato il file shell.php come indicato nell'esercizio:



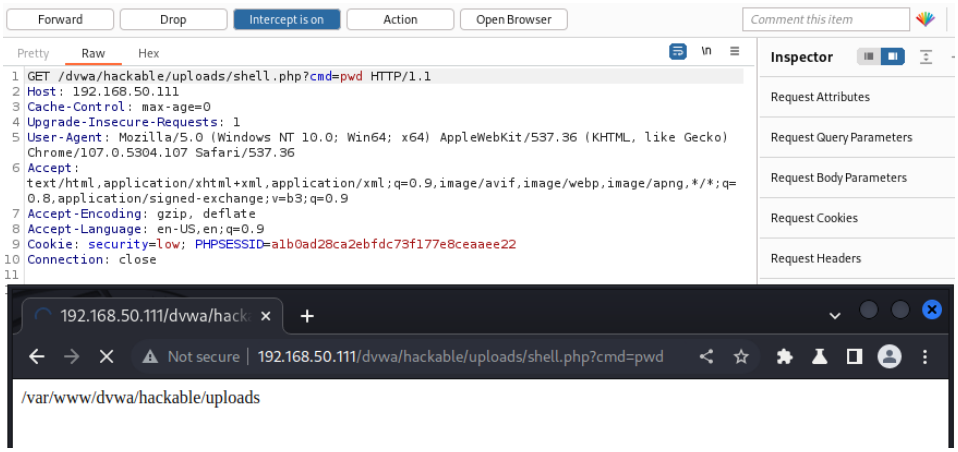
A questo punto ho attivato l'intercettazione di Burpsuite e ho inserito nell'URL il seguente indirizzo: http ://192.168.50.111/dvwa/hackable/uploads/shell.php e il risultato è quello che si può vedere nell'immagine qui sotto:



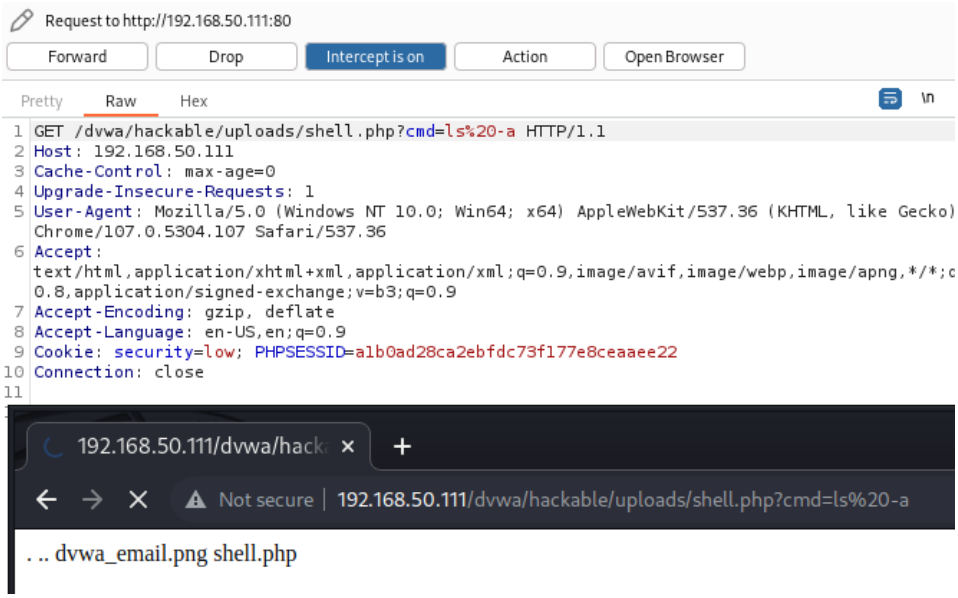
A questo punto ho messo come URL http ://192.168.50.111/dvwa/hackable/uploads/shell.php?cmd=ls attivando la shell caricata precedentemente e attivando il comando ls per vedere i file presenti nella cartella uploads, il tutto mentre intercettavo con Burpsuite:



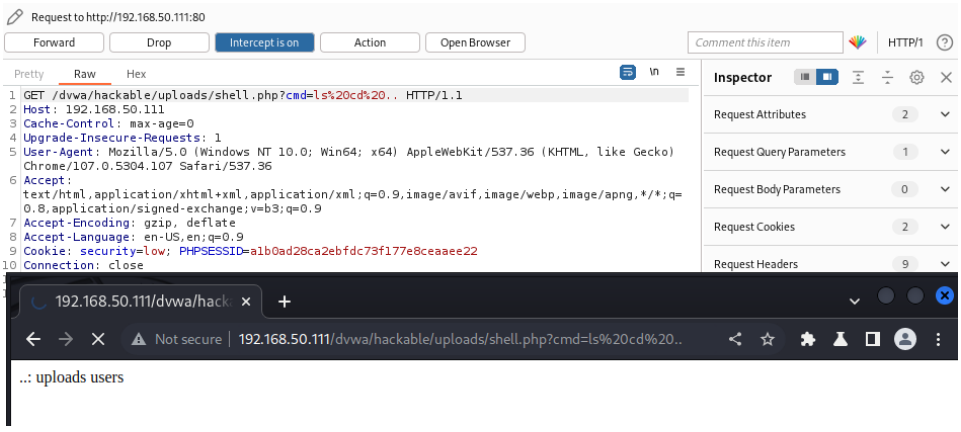
Successivamente ho provato ad utilizzate altri comandi come si può vedere nelle immagini che seguono:



Qui ho usato il comando pwd per vedere il path della shell che abbiamo caricato



Qui invece ho usato il comando ls -a per vedere i file nascosti



Qui invece ho usato il comando ls unitamente al comand cd .. per poter vedere il contenuto della cartella hackable

Ho provato a cambiare il livello di sicurezza, mettendo prima medium e poi high ma non ho riscontrto differenze rispetto ad un livello di sicurezza settato su low.