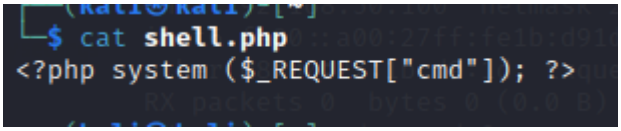
Traccia:

Configurate il vostro laboratorio virtuale in modo tale che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux. Assicuratevi che ci sia comunicazione tra le due macchine.

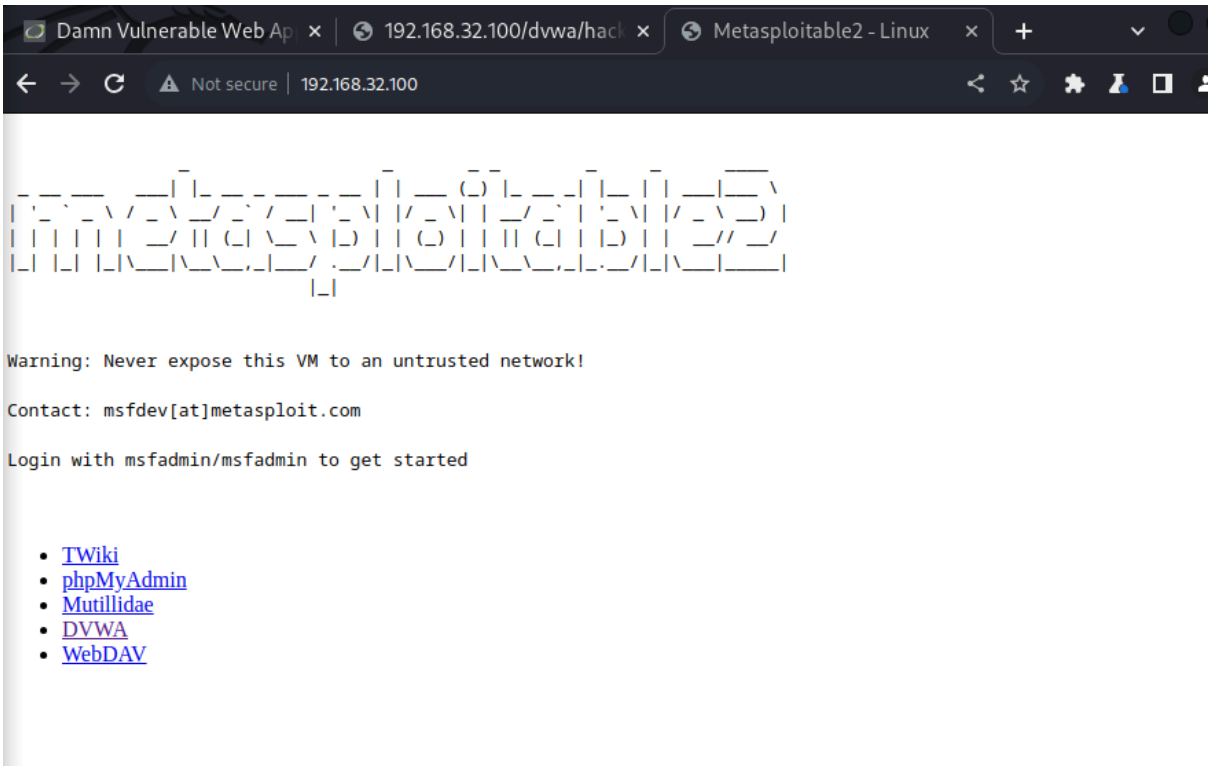
Lo scopo dell'esercizio di oggi è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP.

Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo di intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite.

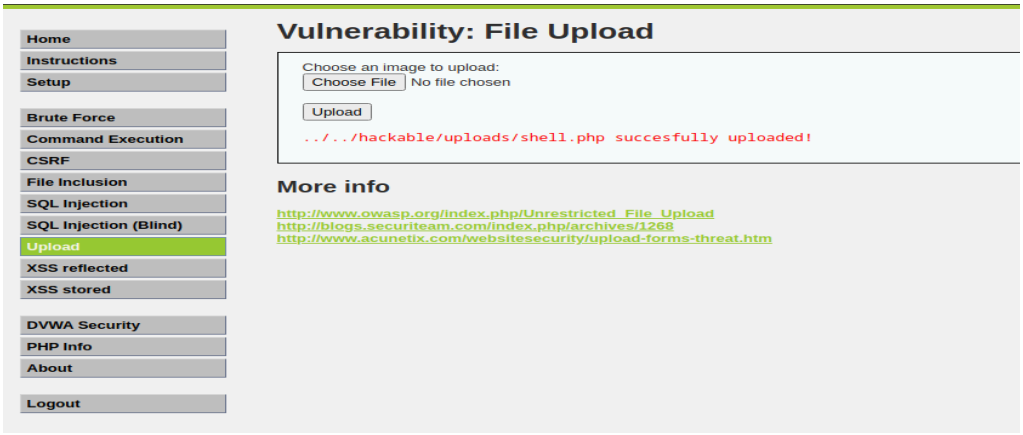
Per prima cosa coso andato a creare un file php chiamato shell.php.

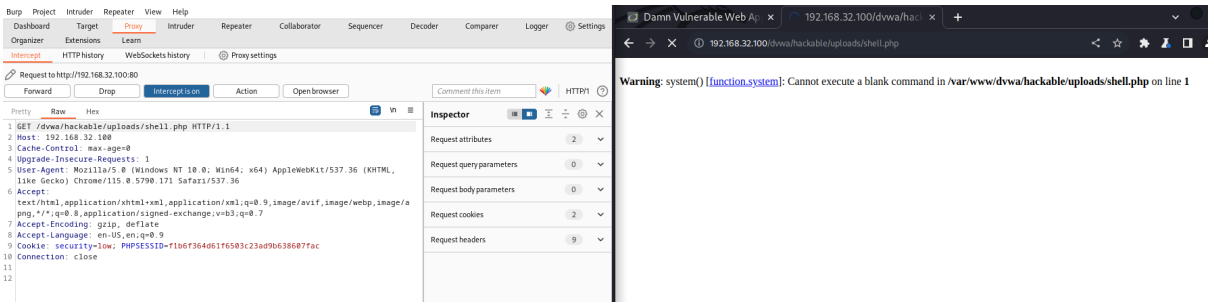


Successivamente ho aperto Burpsuite per controllare le richieste e al suo browser sono entrato nella pagine di metasploitable.

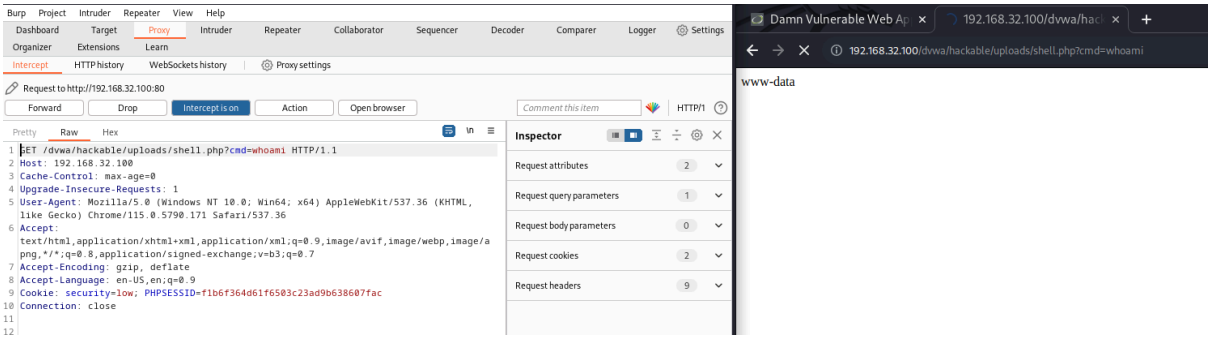


A questo punto sono entrato nella DVWA di meta, ho eseguito l'accesso e ho caricato in upload il file shell.php.

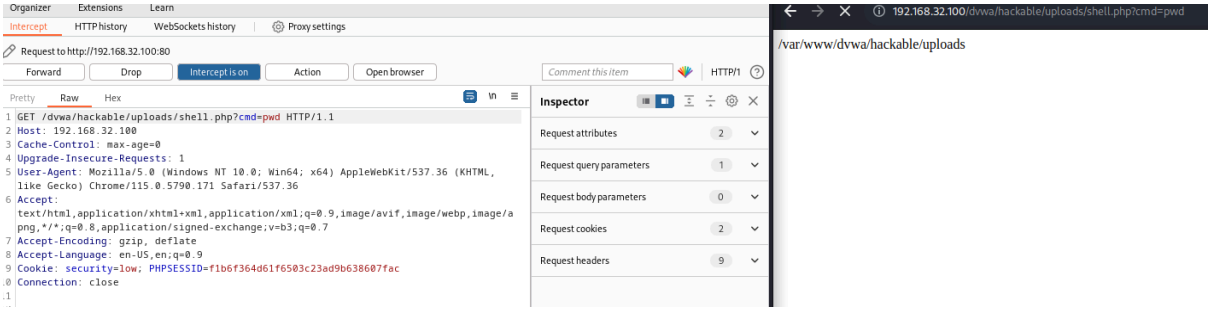




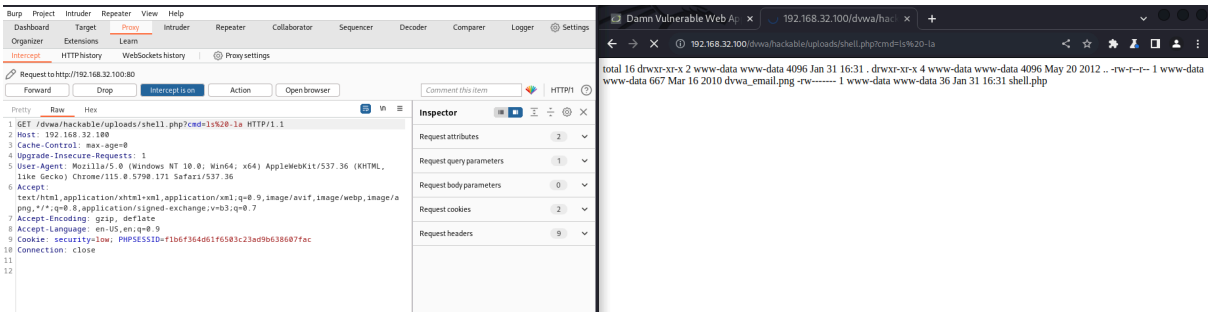
Dopo aver eseguito l'upload ho provato ad eseguire dei comandi per verificare se la shell caricata funzionasse.
whoami:



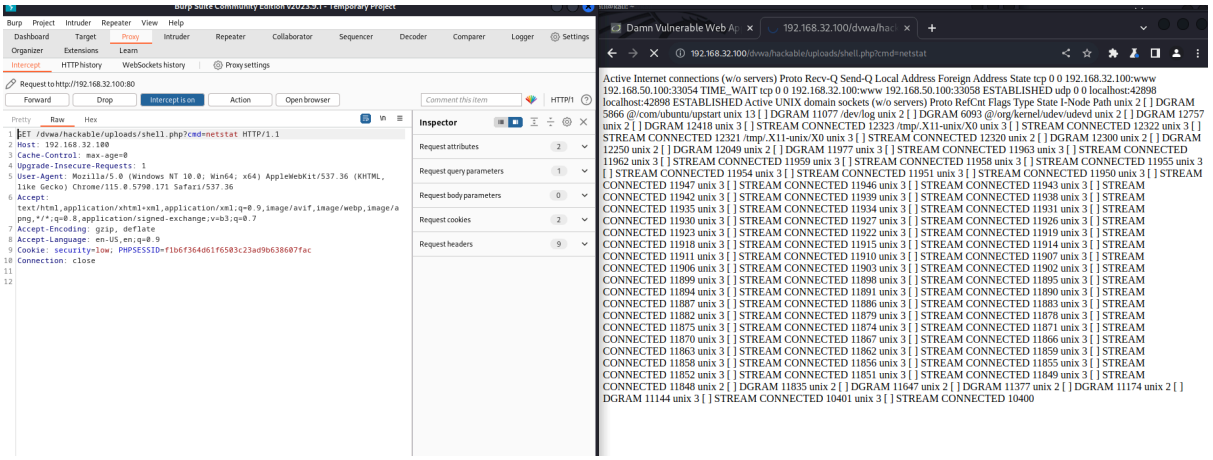
pwd:



ls -la per vedere i file nascosti e le autorizzazioni:



Netstat per aver informazioni sullo stato delle connessioni di rete della macchina:



Grazie a Burpsuite abbiamo notato che sono delle richieste get quindi delle vere e proprie richieste web.