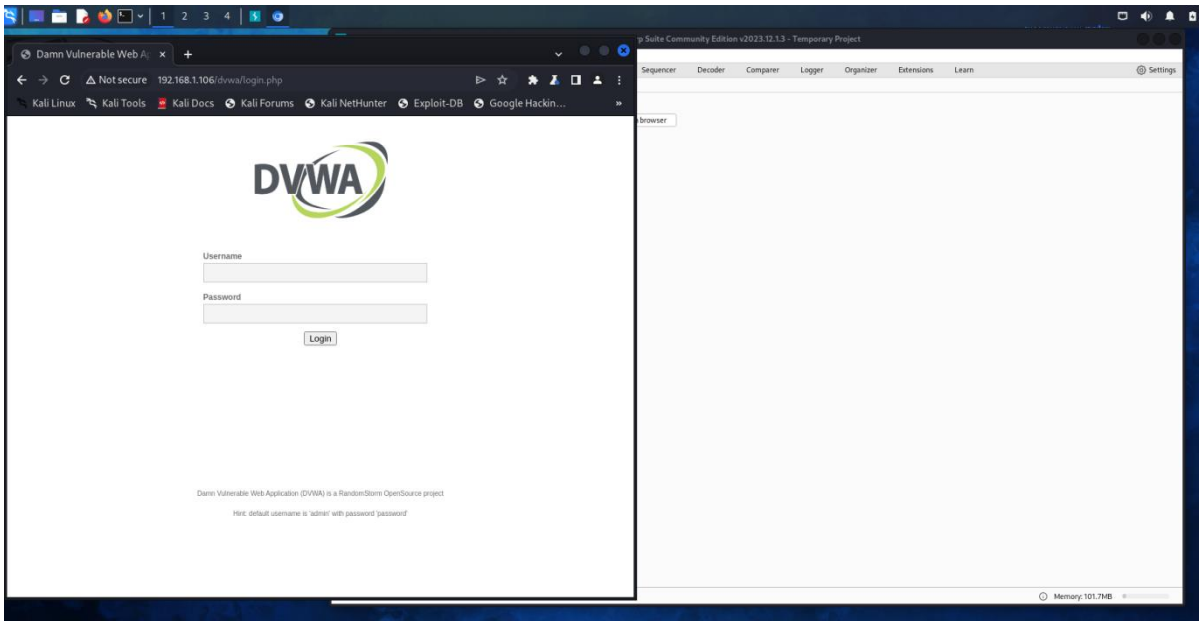
ESERCIZIO W13D1 PRATICA 1

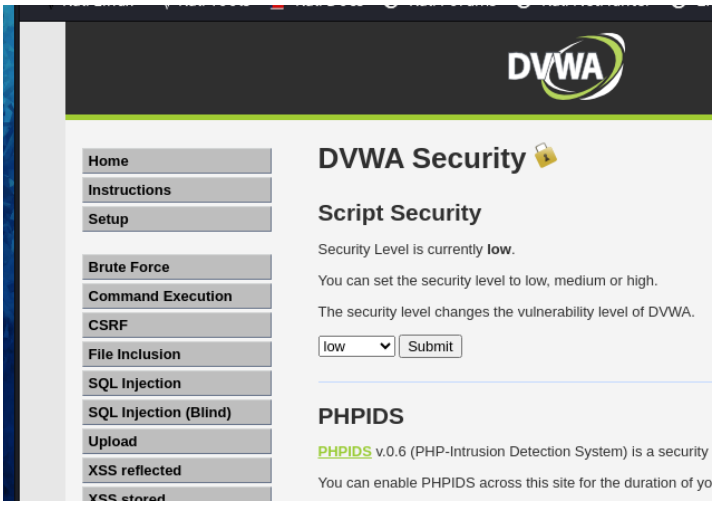
Traccia: Configurate il vostro laboratorio virtuale in modo tale che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux. Assicuratevi che ci sia comunicazione tra le due macchine. Lo scopo dell'esercizio di oggi è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per 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.

SVOLGIMENTO

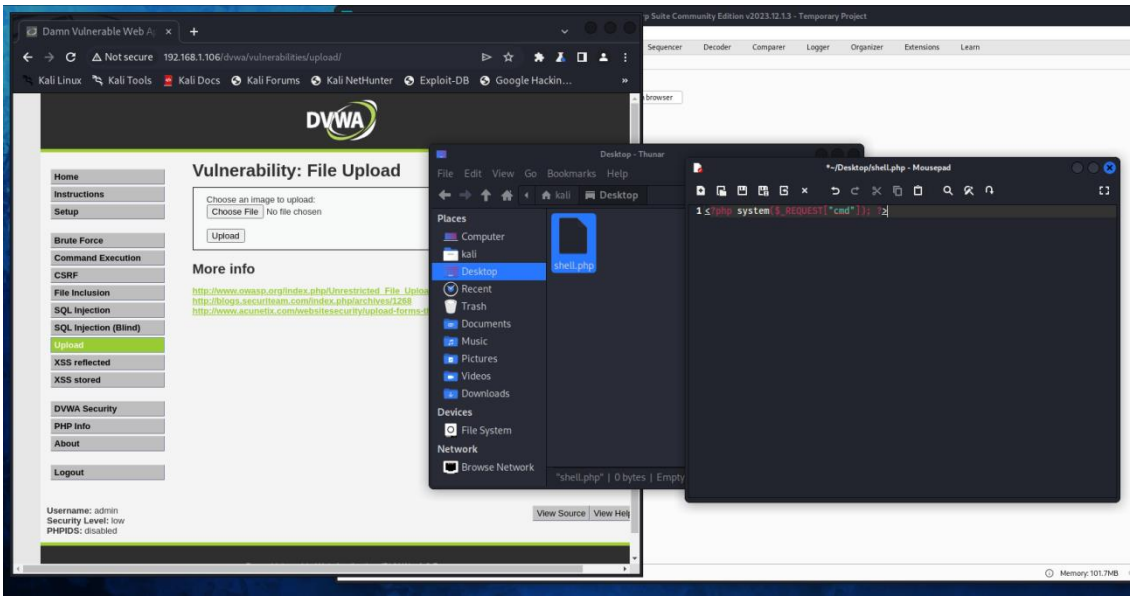
Dopo aver configurato le macchina kali e meta con ip statici e aver visto che pingano, apro burpsuite ed entro nella dvwa tramite ip di meta.



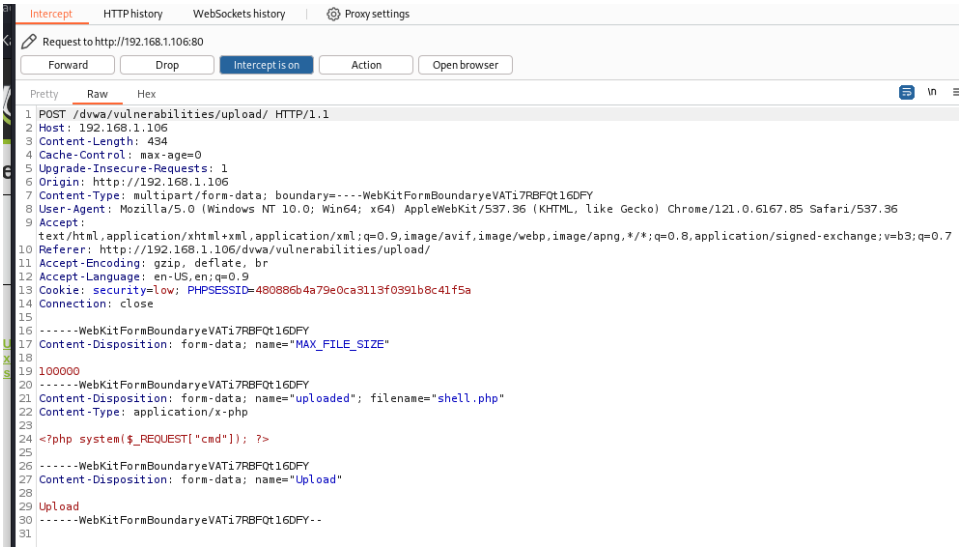
Imposto il livello di sicurezza su low

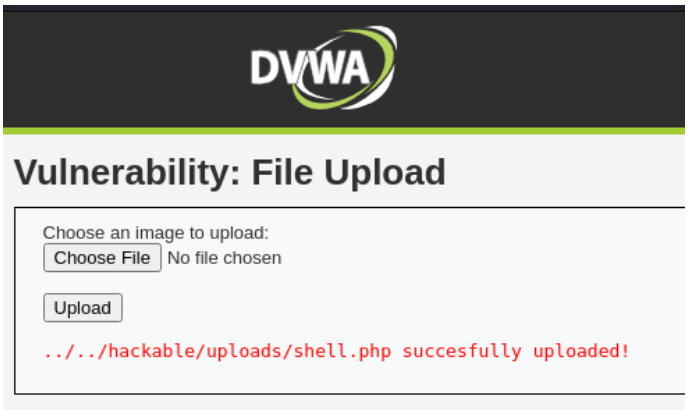


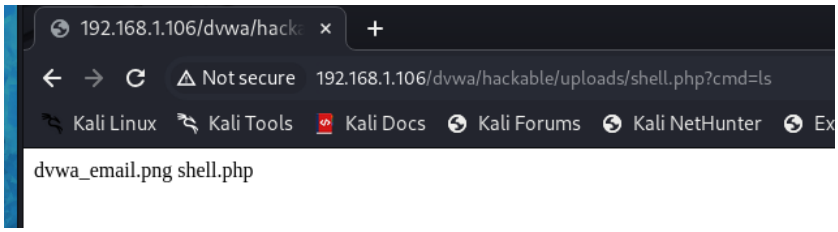
Creo la shell.php con un codice semplice, e dopo aver creato il file lo carico su upload



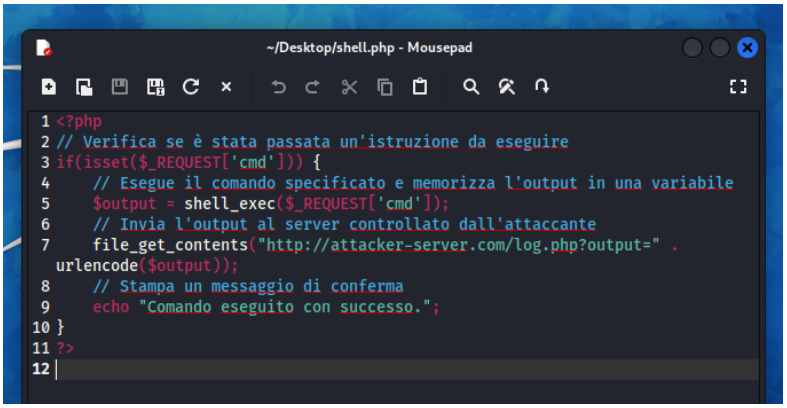
Dopo averla caricata intercetto il traffico con burpsuite e notiamo che la shell è stata caricata correttamente







Dopo di che rieseguo lo stesso esercizio con una shell piu' complessa



Dopo averla caricata, inserisco il comando "?cmd=ls%20-la"che è un modo per passare il comando "ls -la" come parametro nella richiesta HTTP all'URL della shell PHP, così che la shell eseguirà quel comando e restituirà l'output della directory corrente e dei file ad essa associati.