In questa lezione vedremo come sfruttare un file upload sulla DVWA per caricare una semplice shell in PHP. **Monitoreremo tutti gli step con BurpSuite**

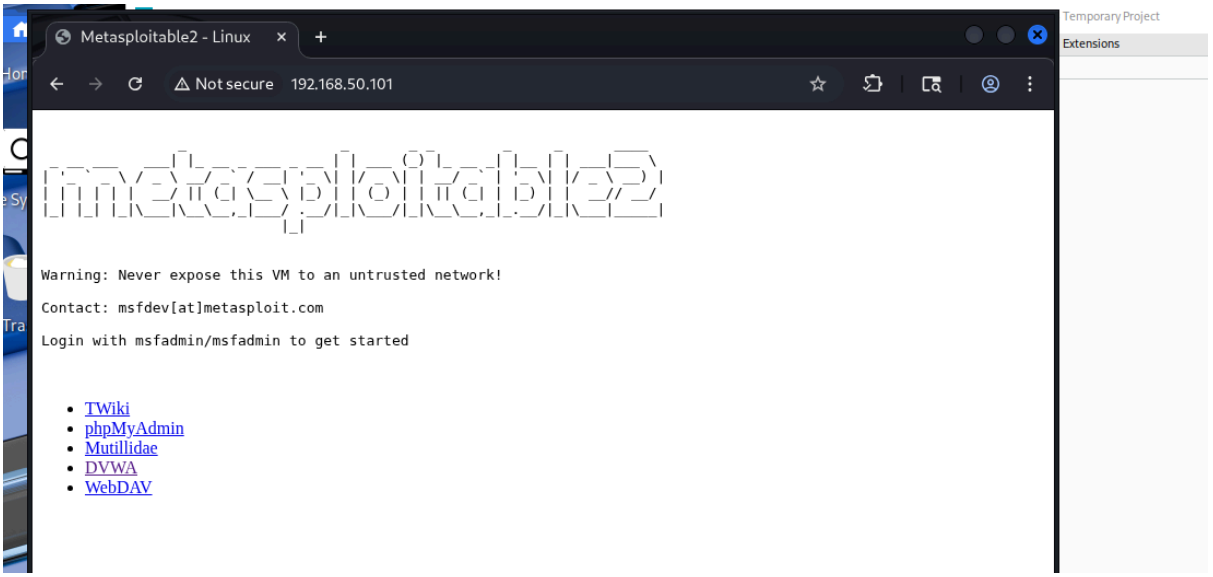
Traccia:

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.

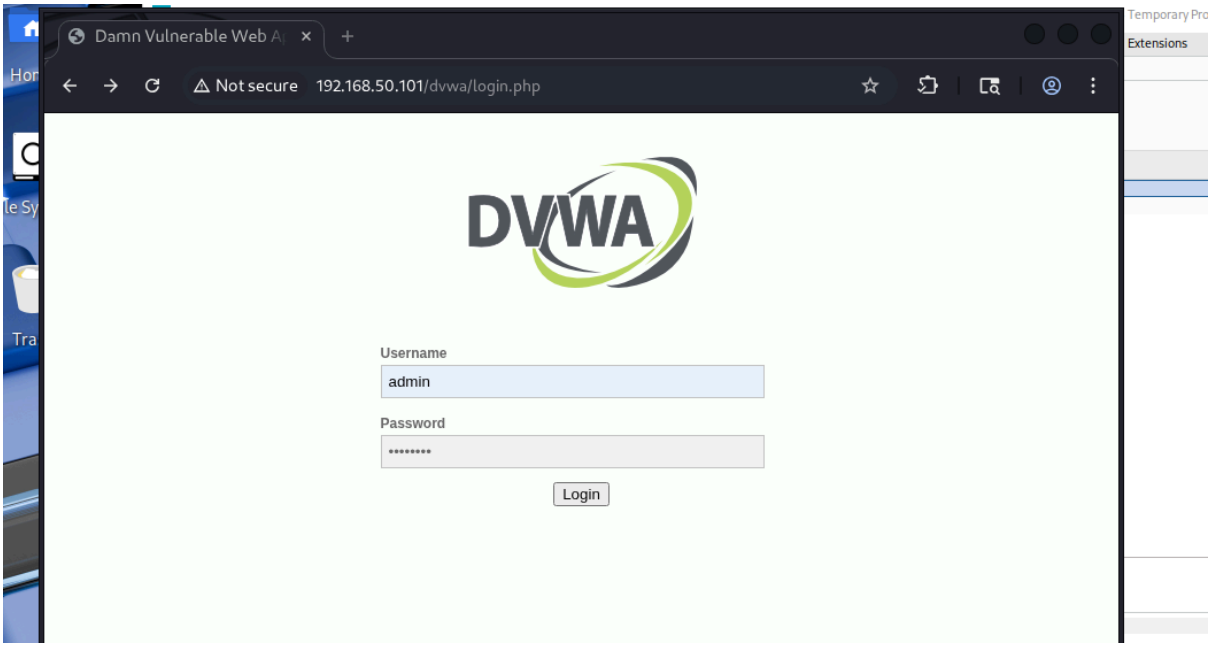
Lo scopo è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP.

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**.

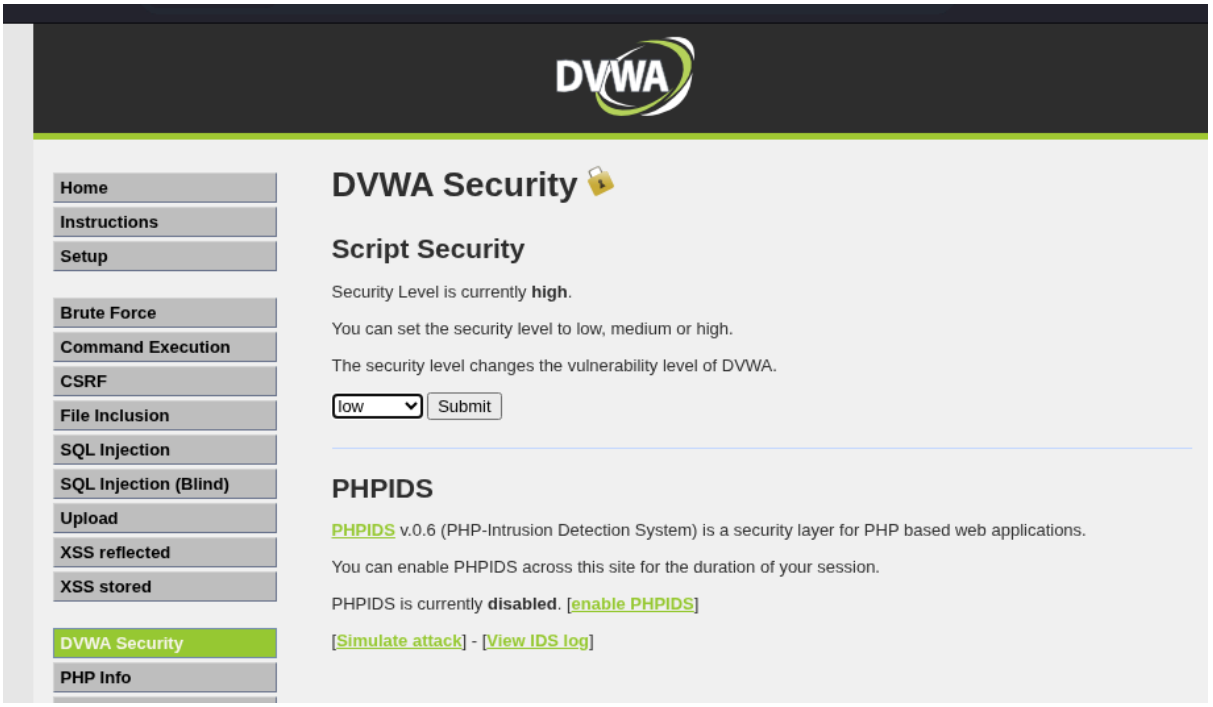
SVOLGIMENTO:



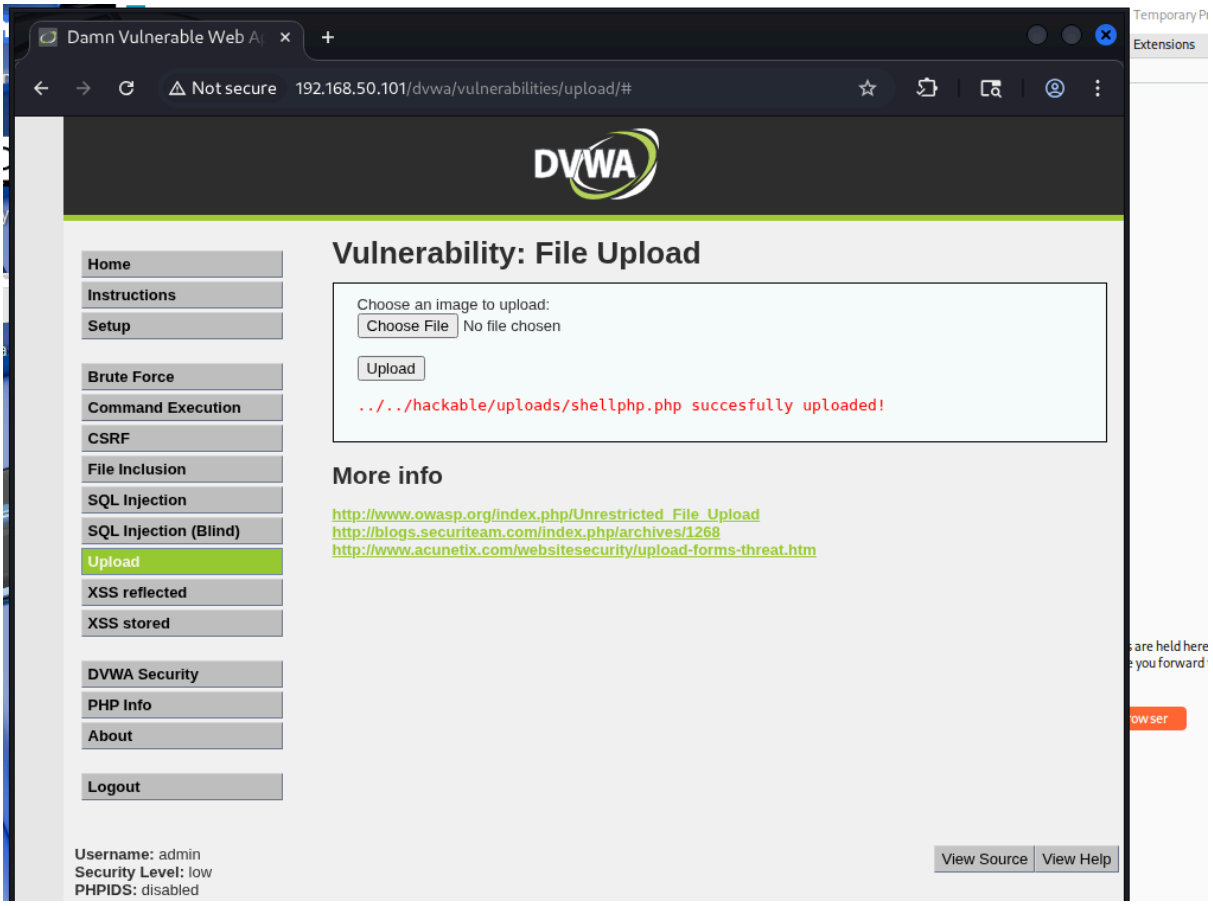
per prima cosa ho attivato burp suite ho messo intercet on e ho aperto il browser mi sono connessa meta e ho selzionato DWVA



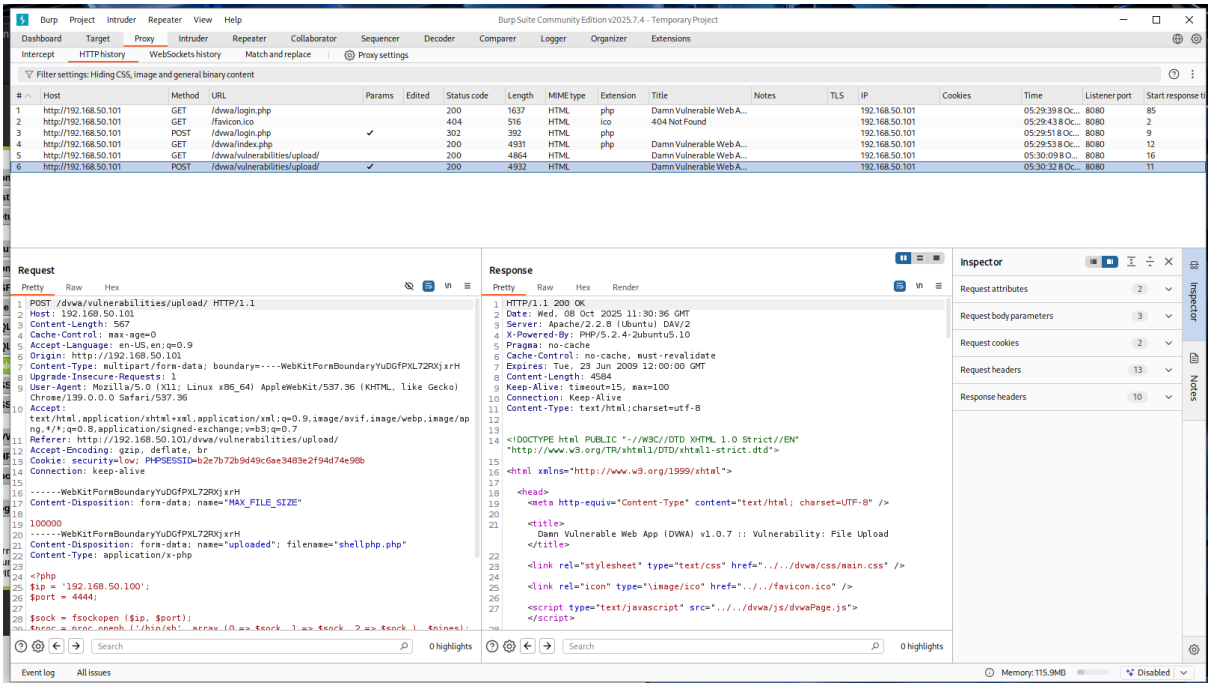
ho effettuato l’accesso con admin e password

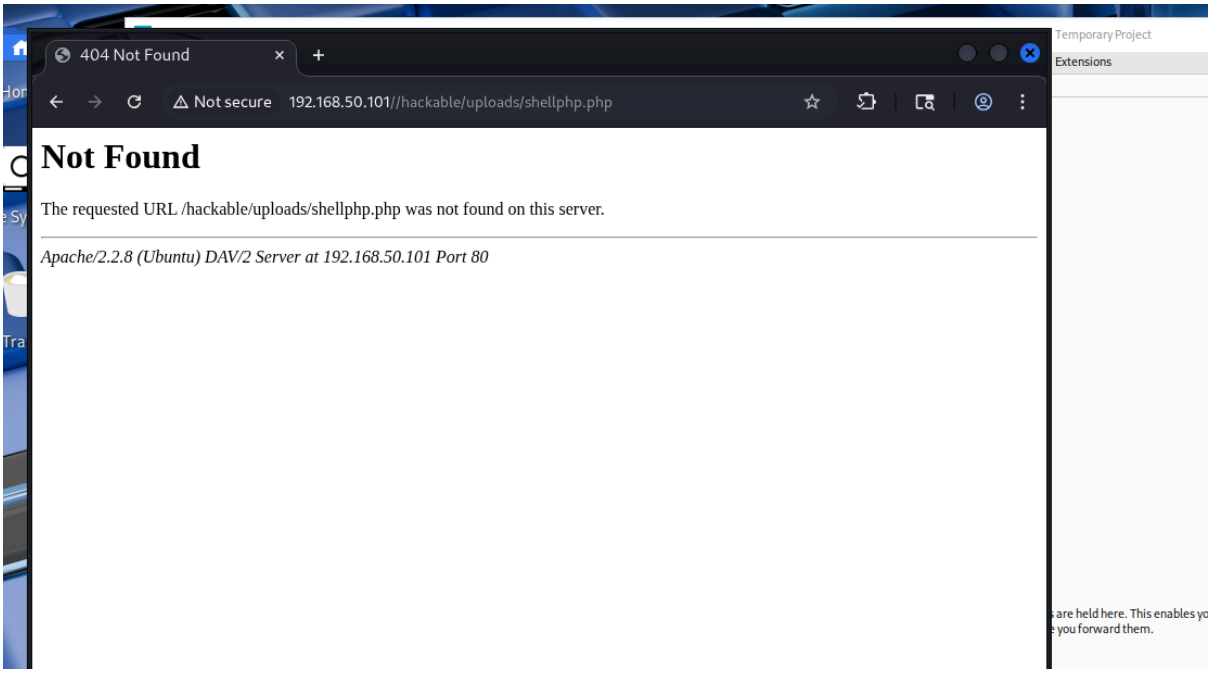


dopo ho impostato il livello di DWVA security a low

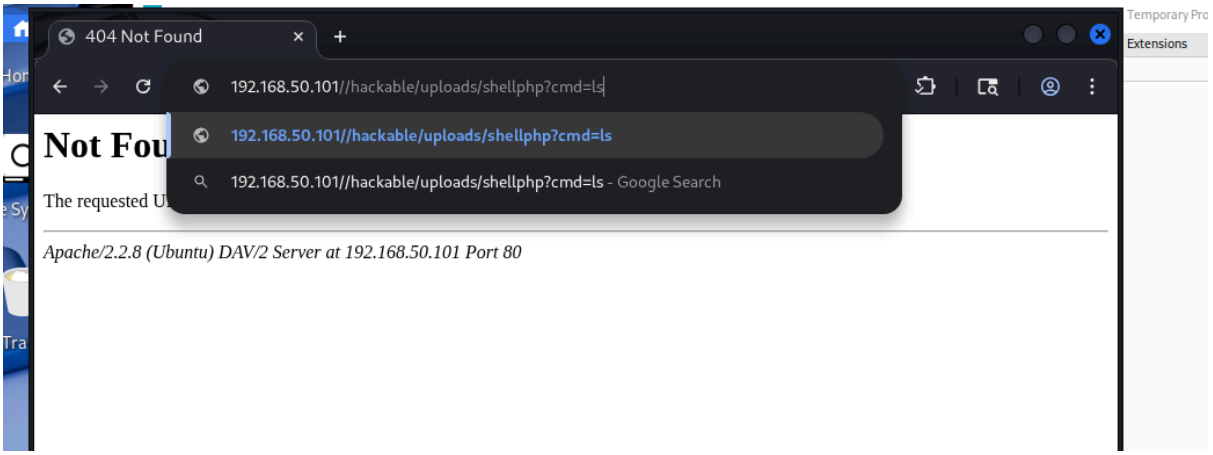


sono andata su upload ho caricato la shell di php





mi sono collegata al path che mi ha dato dopo aver caricato la shell di php e ho ricevuto il seguente messaggio di errore Il motivo è che la shell richiede un parametro cmd nella richiesta GET per eseguire un comando, ma non abbiamo ancora passato alcun argomento



adesso possiamo intercettare la richiesta generica e modificarla a nostro piacimento da burp suite.

CODICE PHP