Esercizio S6L1

Traccia:

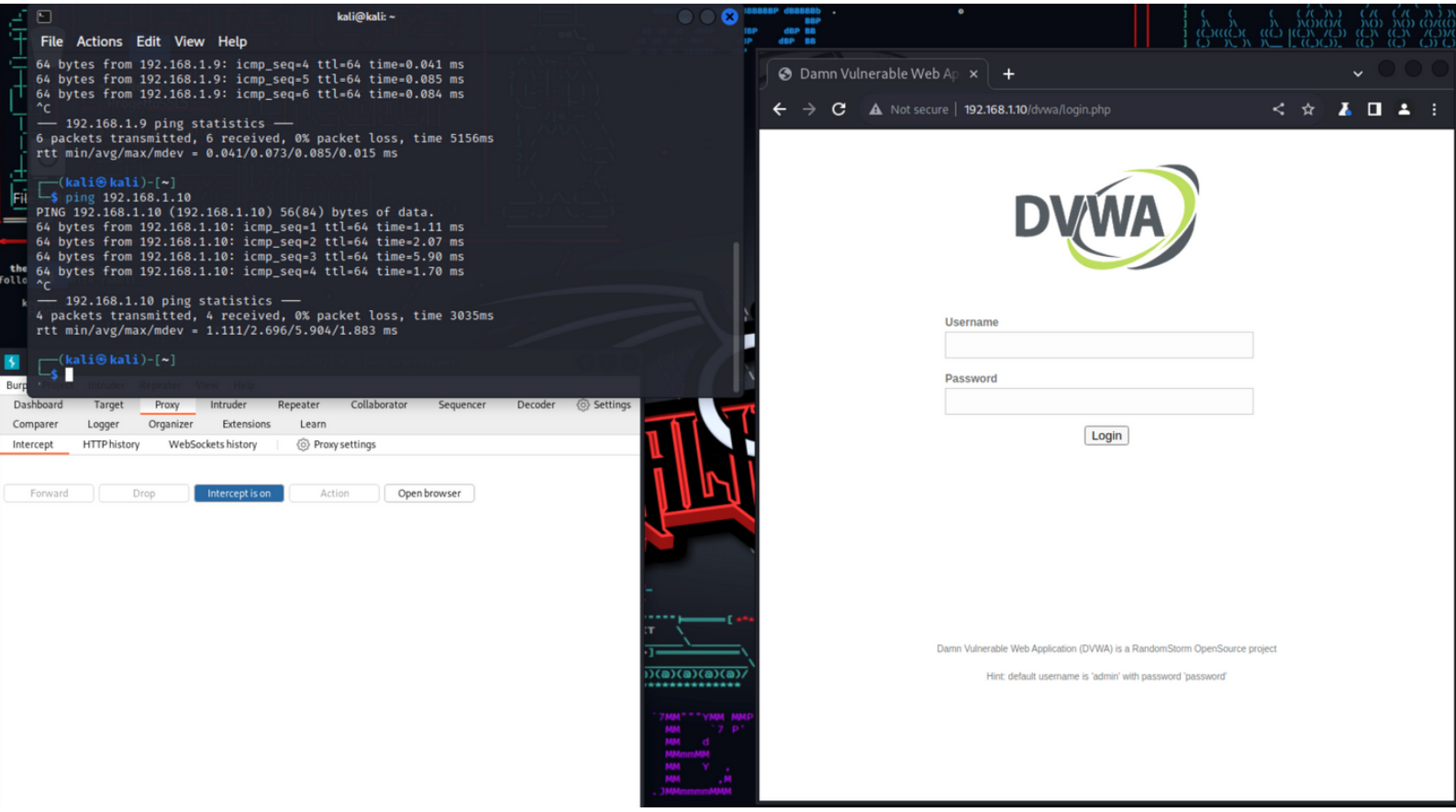
Configurate il vostro laboratorio virtuale in modo tale che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux. Assicuratevi che ci sia comunicazione tra le due macchine.

Lo scopo dell'esercizio 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**.

1) Controllo della comunicazione tra Kali Linux e Metasploitable

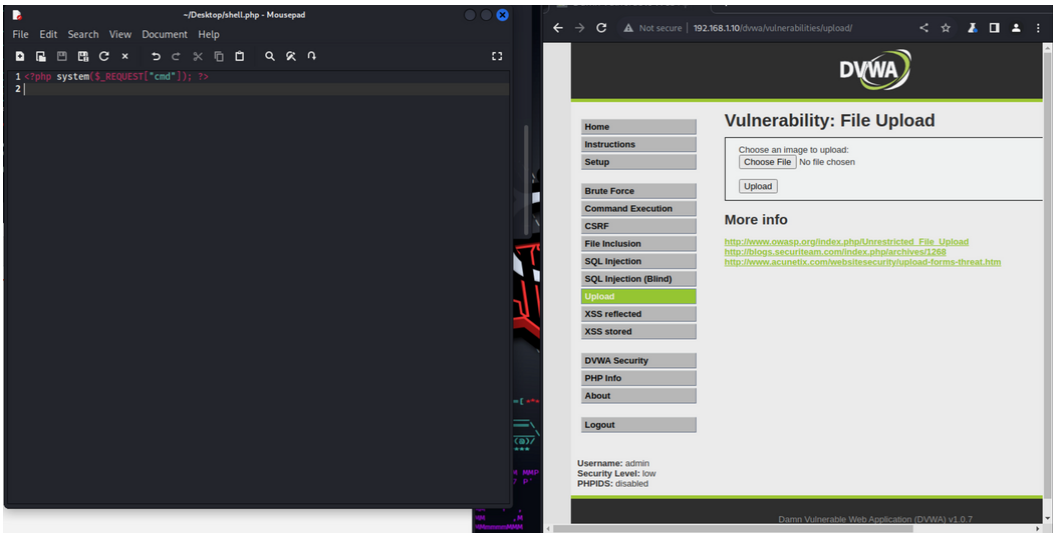
2) Fare l'accesso a DVWA nel browser di Burp Suite

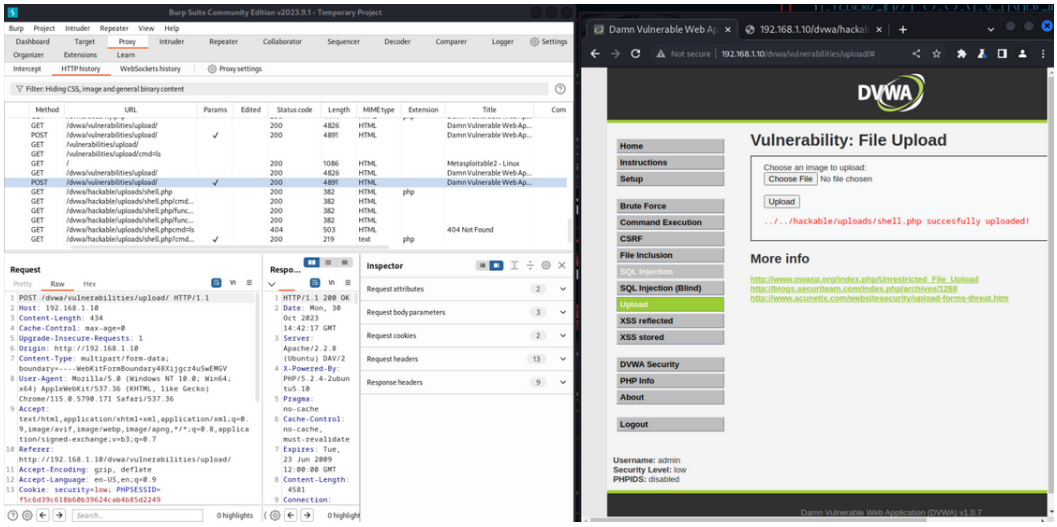


3) Creare un file php contenente il codice seguente “<?php system($_REQUEST["cmd"]); ?>”

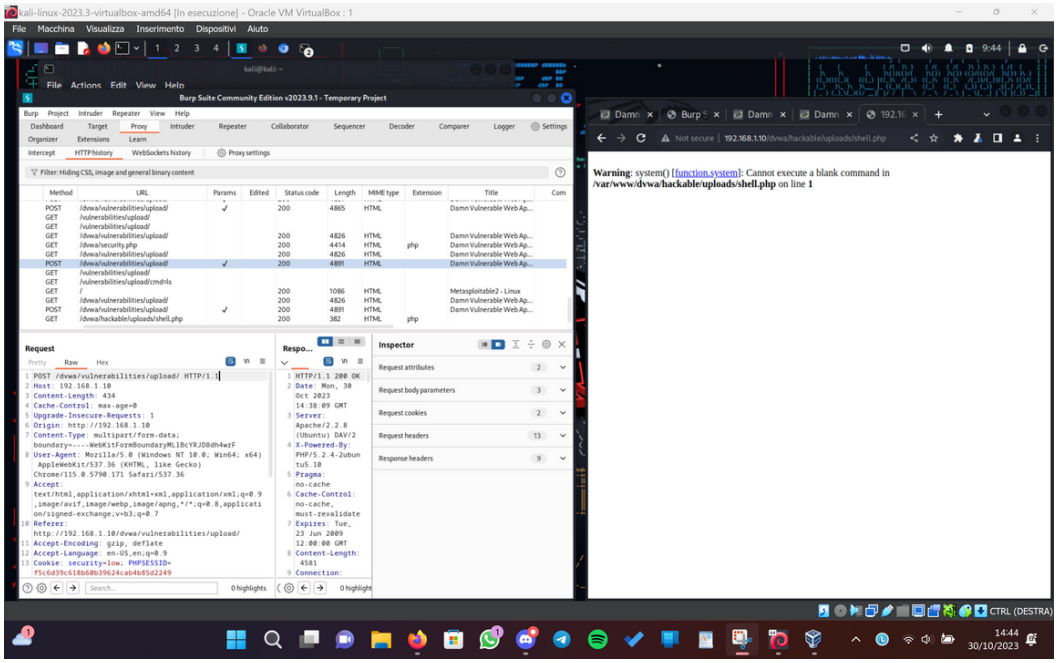
4) Configurare la sicurezza in quella più bassa per far si che l’esercizio vada a buon fine

5) Caricare il file creato nel punto 3

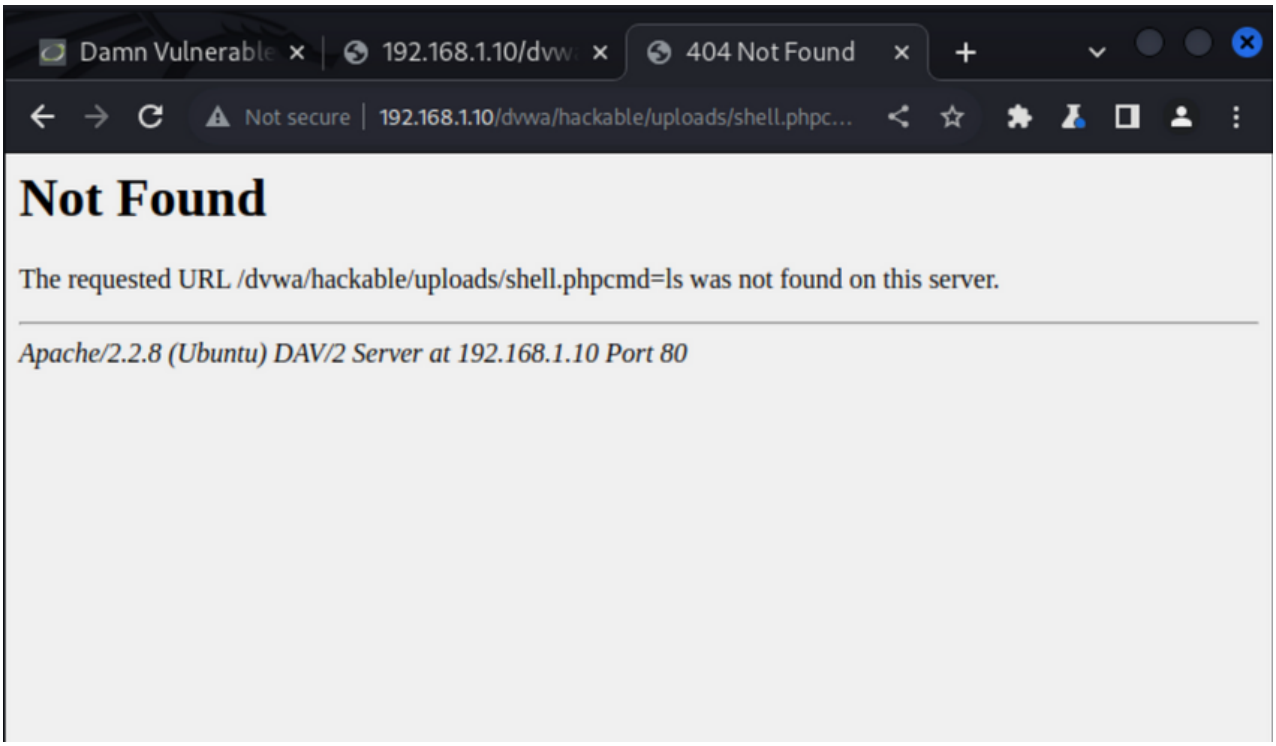




6) Copiare il percorso che ha creato DVWA non appena si ha caricato il file php e incollare nella barra di ricerca dopo aver scritto: indirizzo ip di Metasploitable/dvwa/percorso creato ma non andrà bene perchè manca un comando all’interno del codice del file



quindi abbiamo scritto il comando direttamente nell'URL senza modificare il file ma ci dava comunque un errore cioè quello di non aver separato il percorso dal comando



come soluzione per separare abbiamo usato il ?