RELAZIONE S6L1

TRACCIA

EPICODE

Pratica S6/L1 PDF

Esercizio
Traccia

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

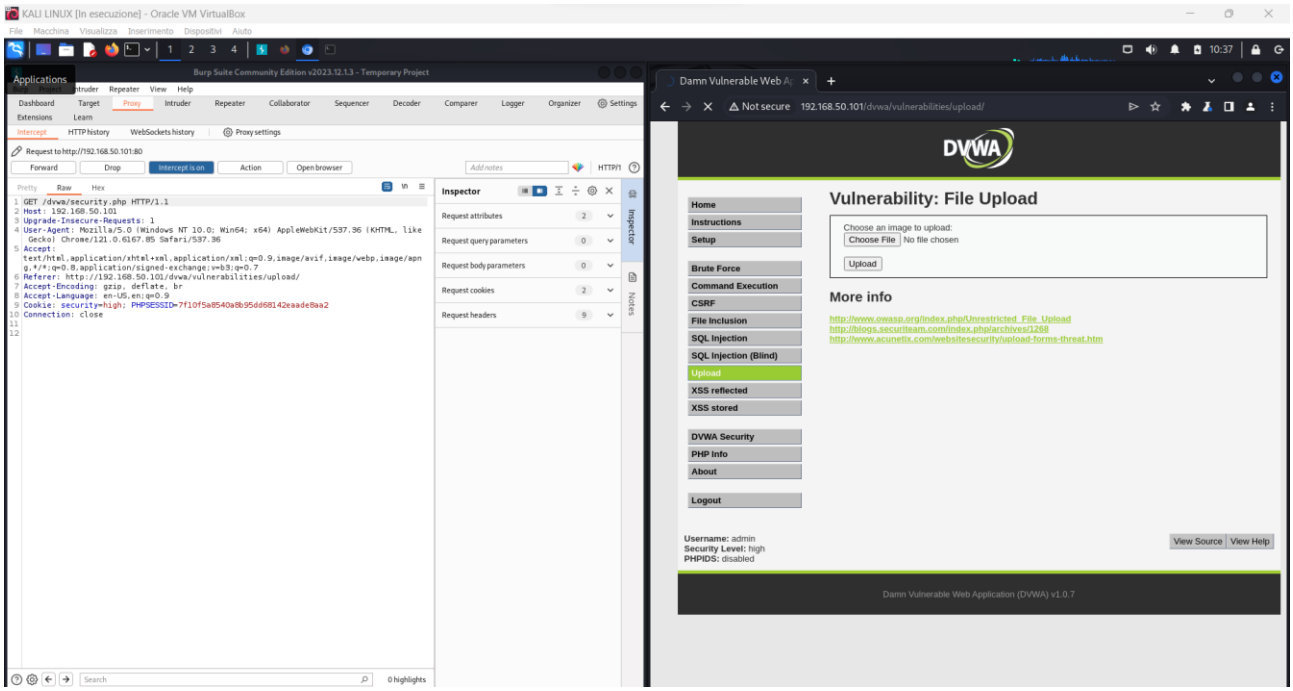
Traccia:

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.

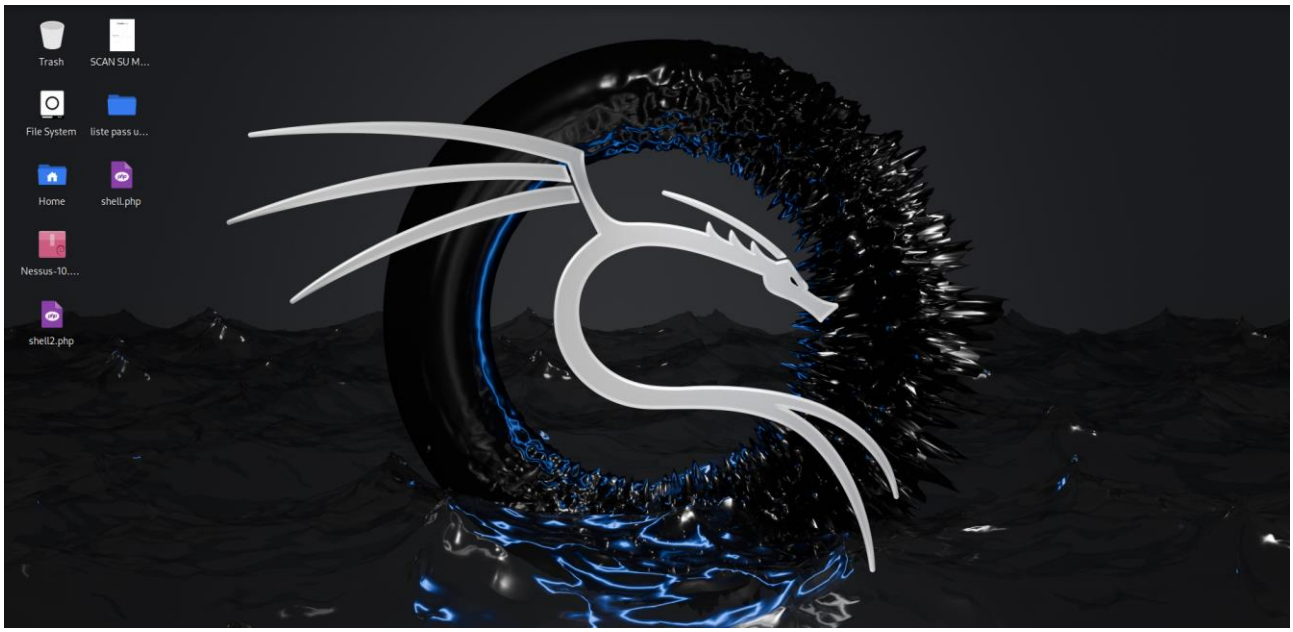
Lo scopo dell'esercizio di oggi è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP. Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo **di intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite**.

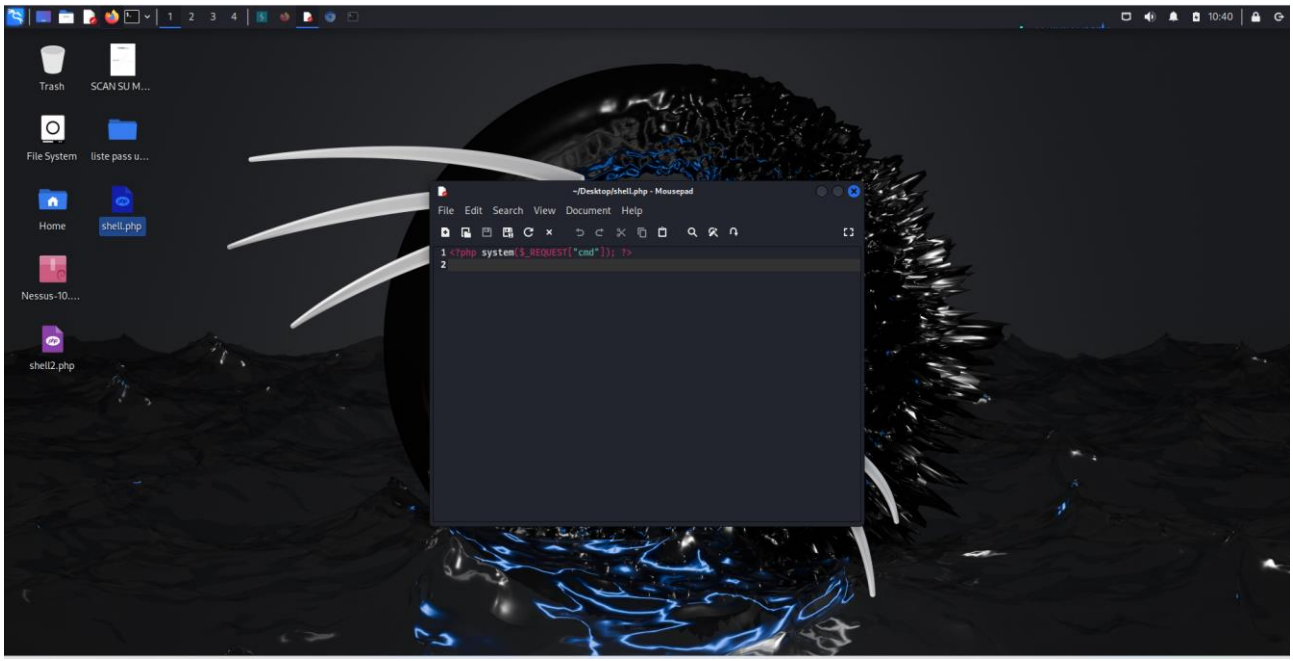
"RISOLUZIONE"

COLLEGAMENTO CON BURP SUITE



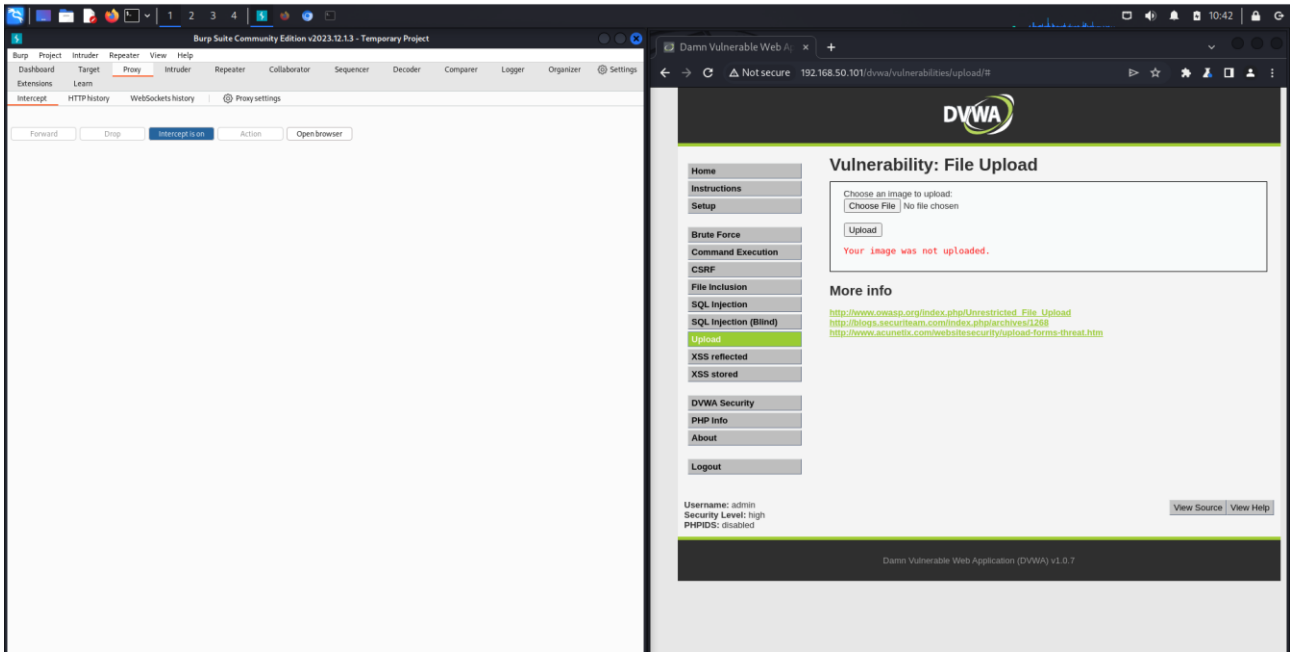
In questa fase abbiamo creato un collegamento con la dvwa di metasploitable. Nella quale andreamo a caricare la nostra shell.php creata in precedenza.

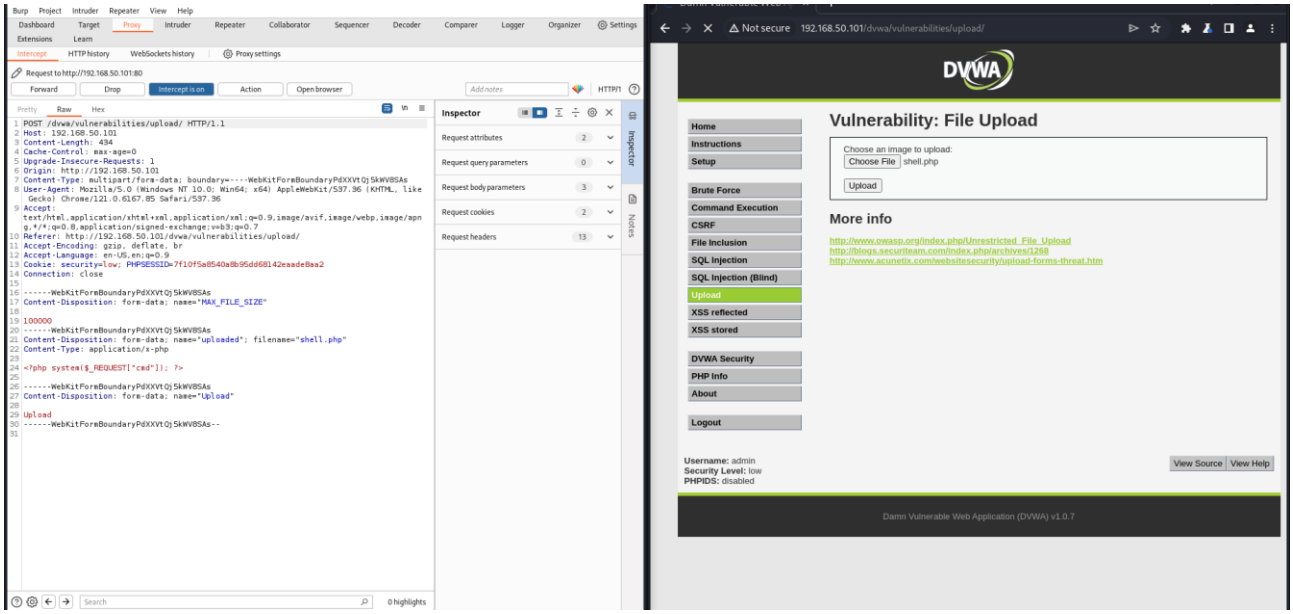




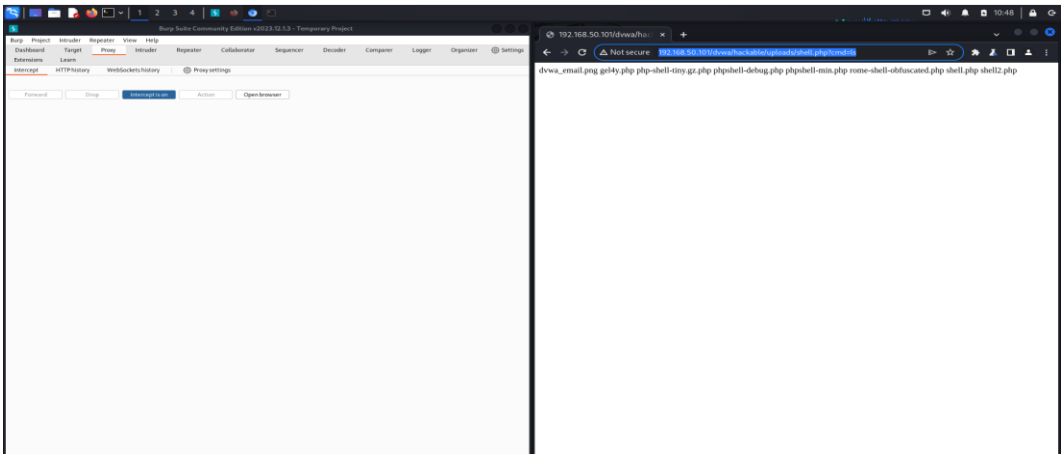
Questa e la riga di comando inserita all'interno della shell che abbiamo creato

Ed ora andiamo a vedere il risultato



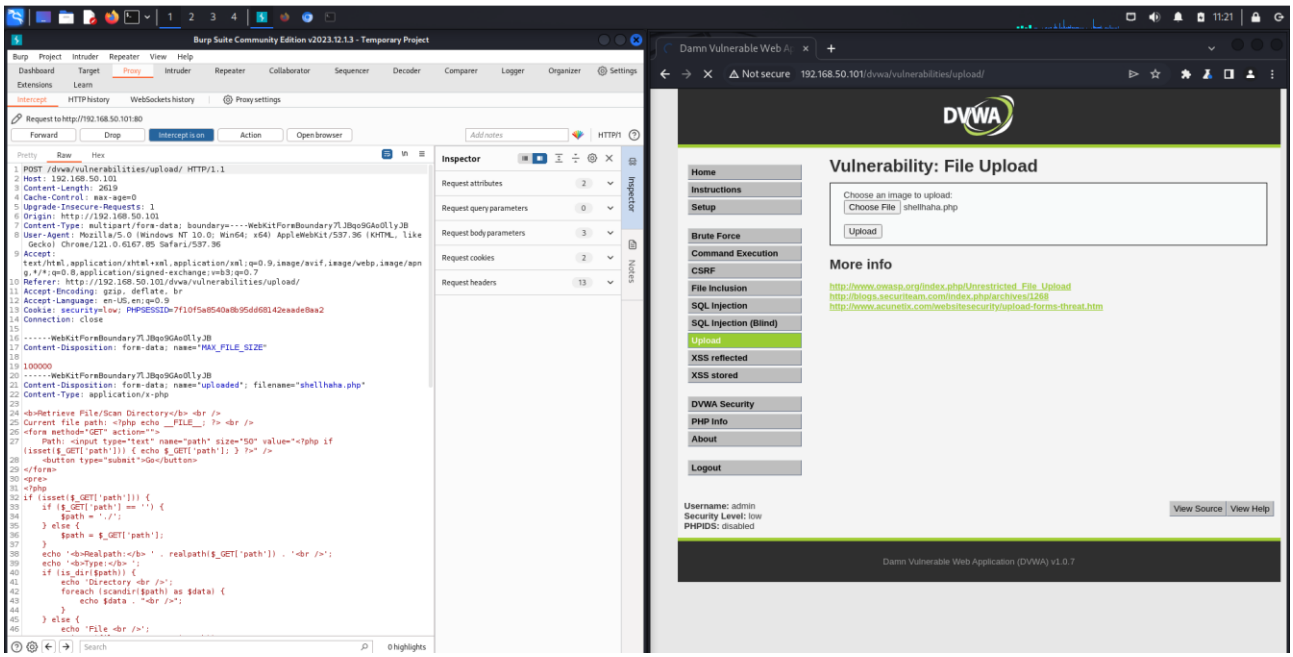


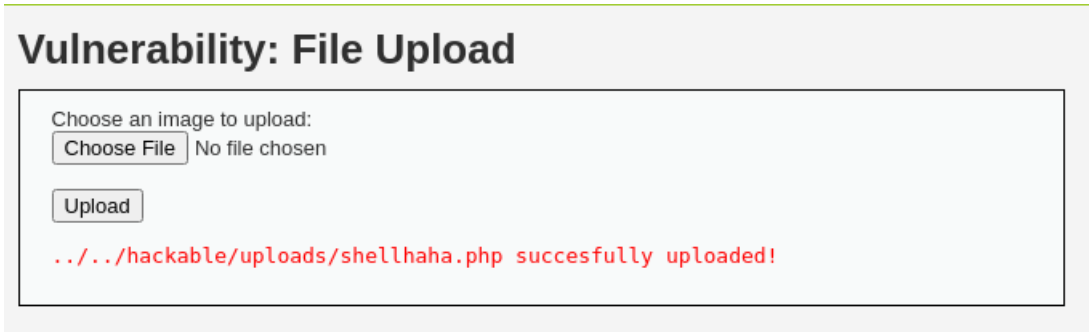
Ed ecco il risultato finale

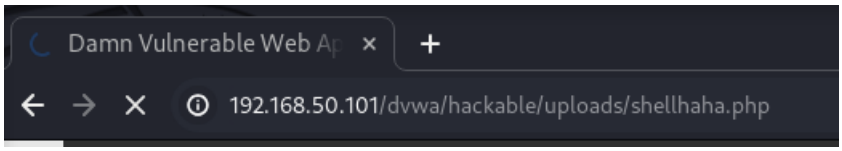


SHELL AVANZATA

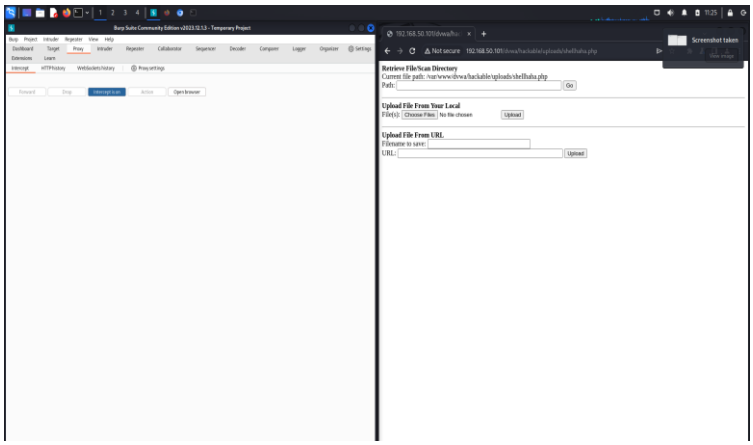
Questa shell ci permette di caricare una shell ed effettuare l'upload presso un url da noi inserito







Ecco il risultato



Questo e il comando del php