26 FEBBRAIO 2024

REPORT - EPICODE

S6L1

PRESENTED BY

Alessandro Marasca

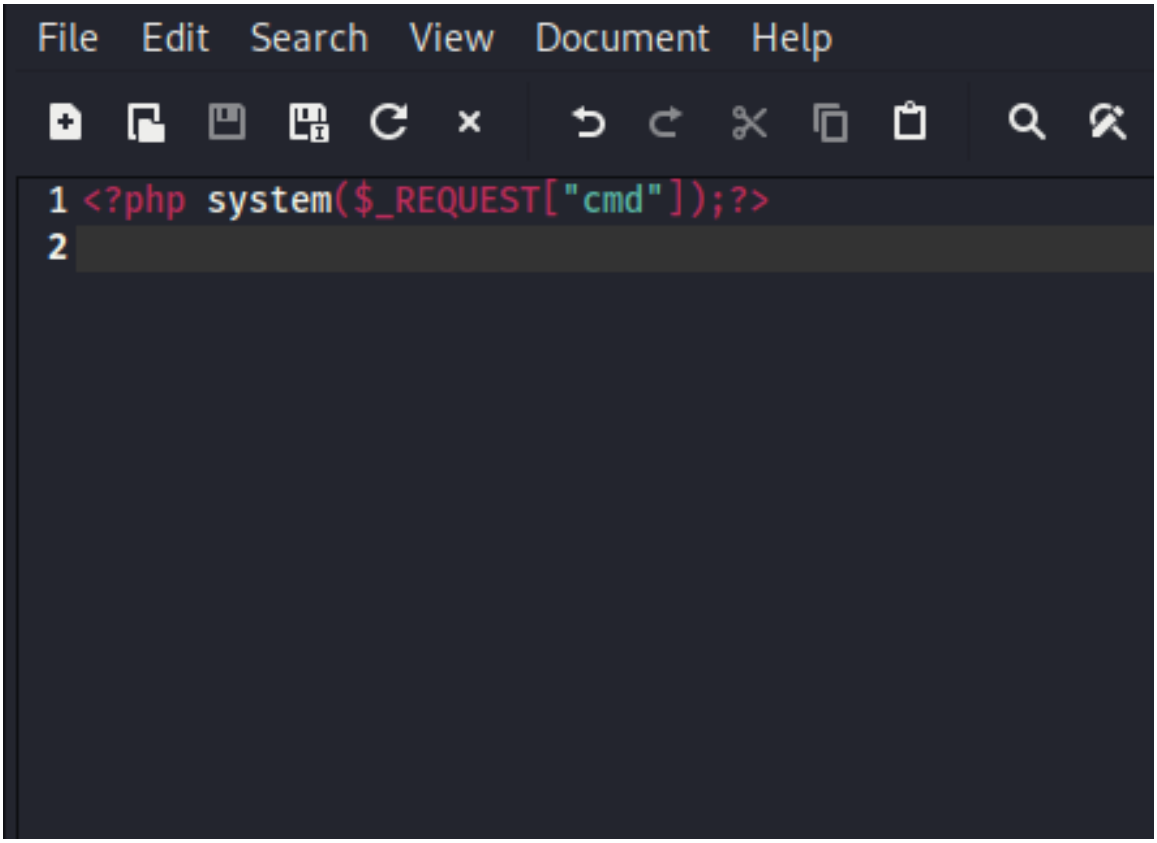
EXPLOIT - FILE UPLOAD TRACCIA

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.

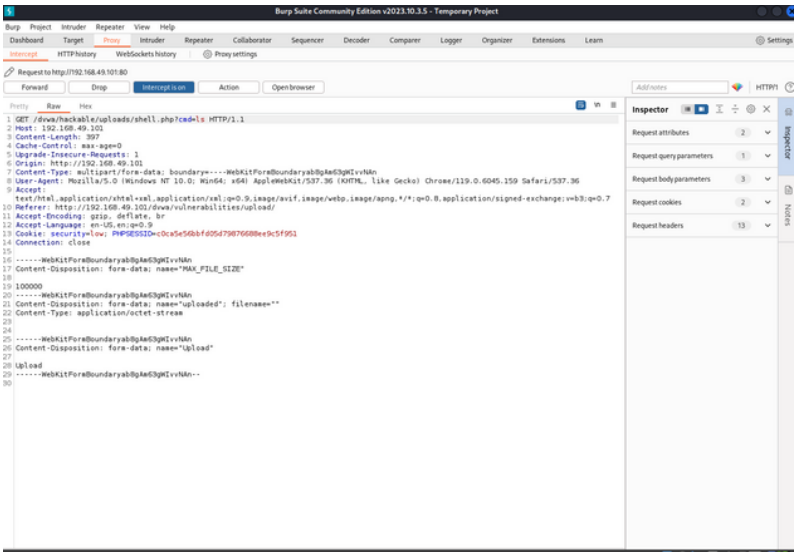
Lo scopo dell'esercizio di oggi è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP. Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo di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

Consegna:
- Codice php.
- Risultato del caricamento (screenshot del browser).
- Intercettazioni (screenshot di burpsuite).
- Risultato delle varie richieste.
- Eventuali altre informazioni scoperte della macchina interna.
- BONUS: usare una shell php più sofisticata.

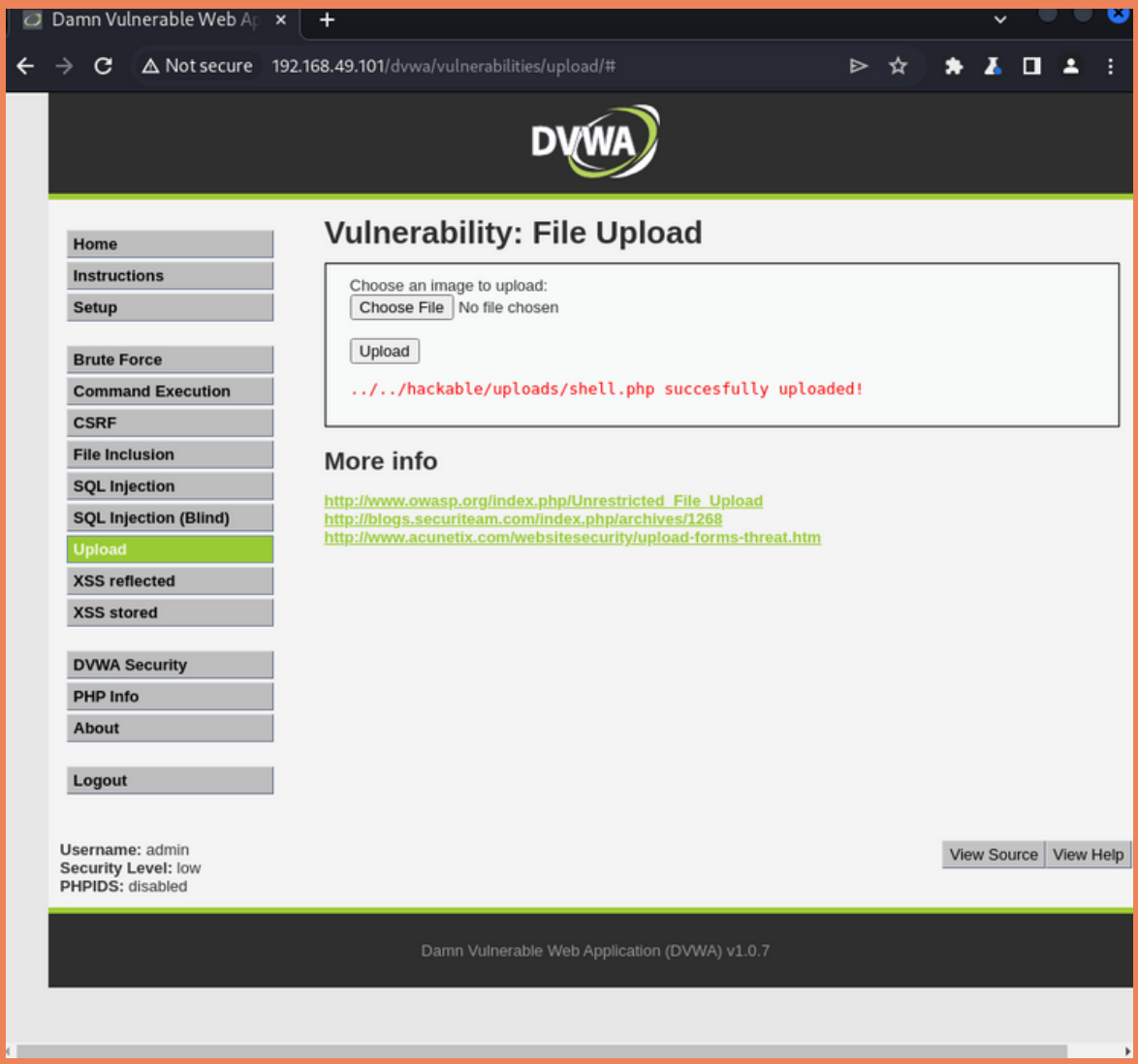
LINEA DI COMANDO PHP



INTERCETTAZIONE BURP SUITE



UPLOAD EFFETTUATO



Alessandro Marasca

Epicode

S6L1- CS0124

26 FEBBRAIO 2024