ESERCITAZIONE W13D1

EPICODE

Esercizio
Traccia

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

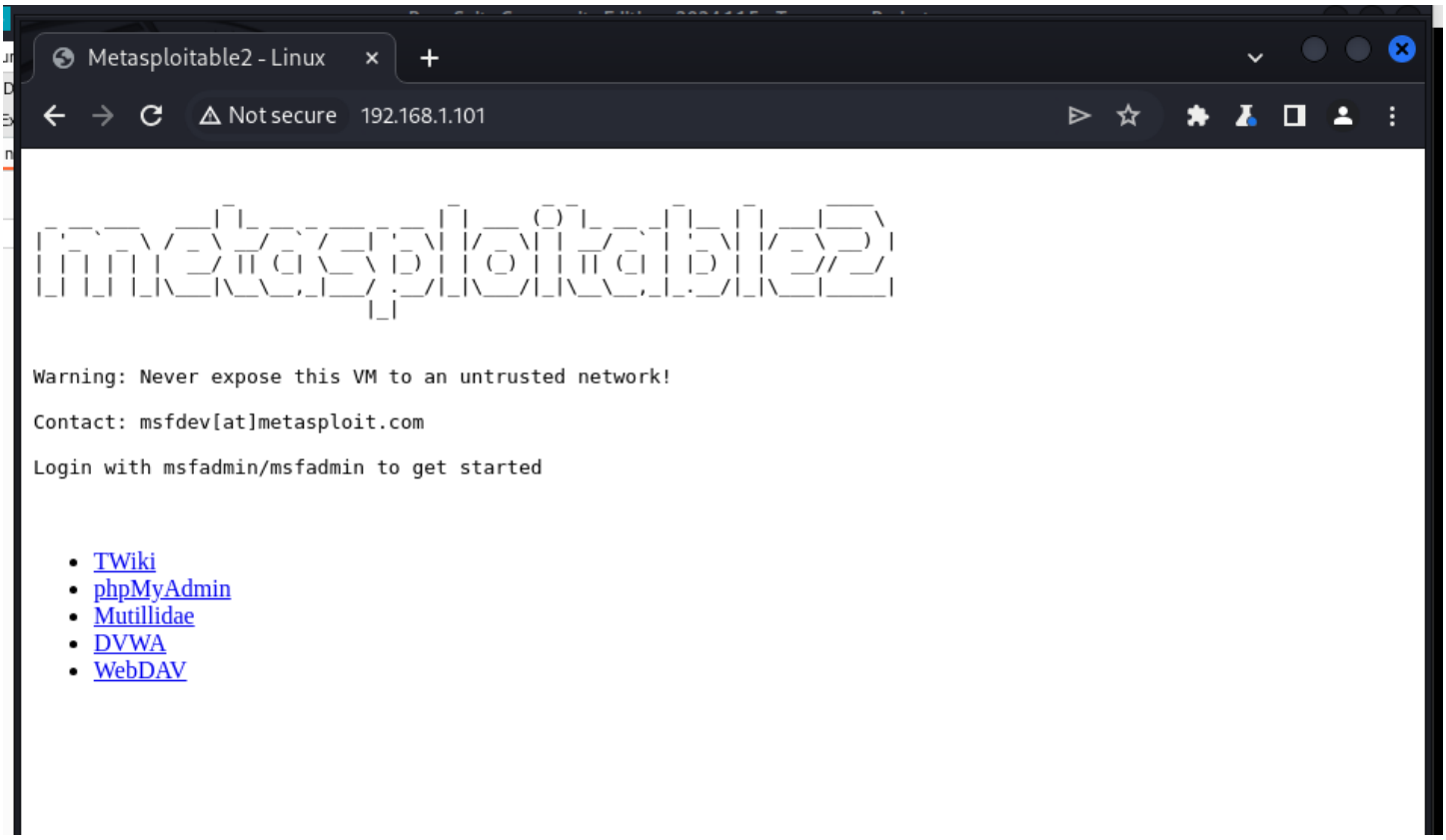
Traccia:

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.

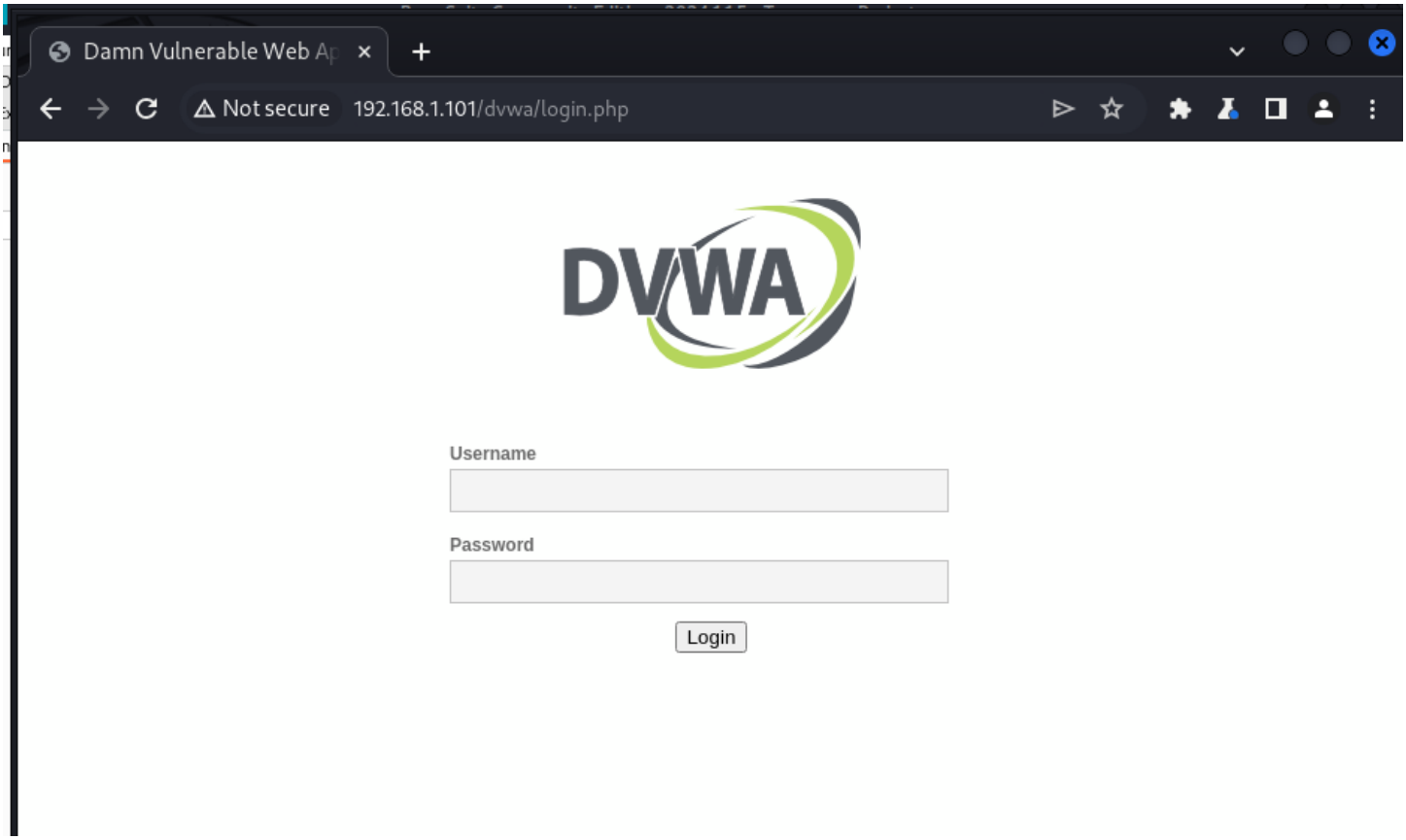
Lo scopo dell'esercizio di oggi è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP.

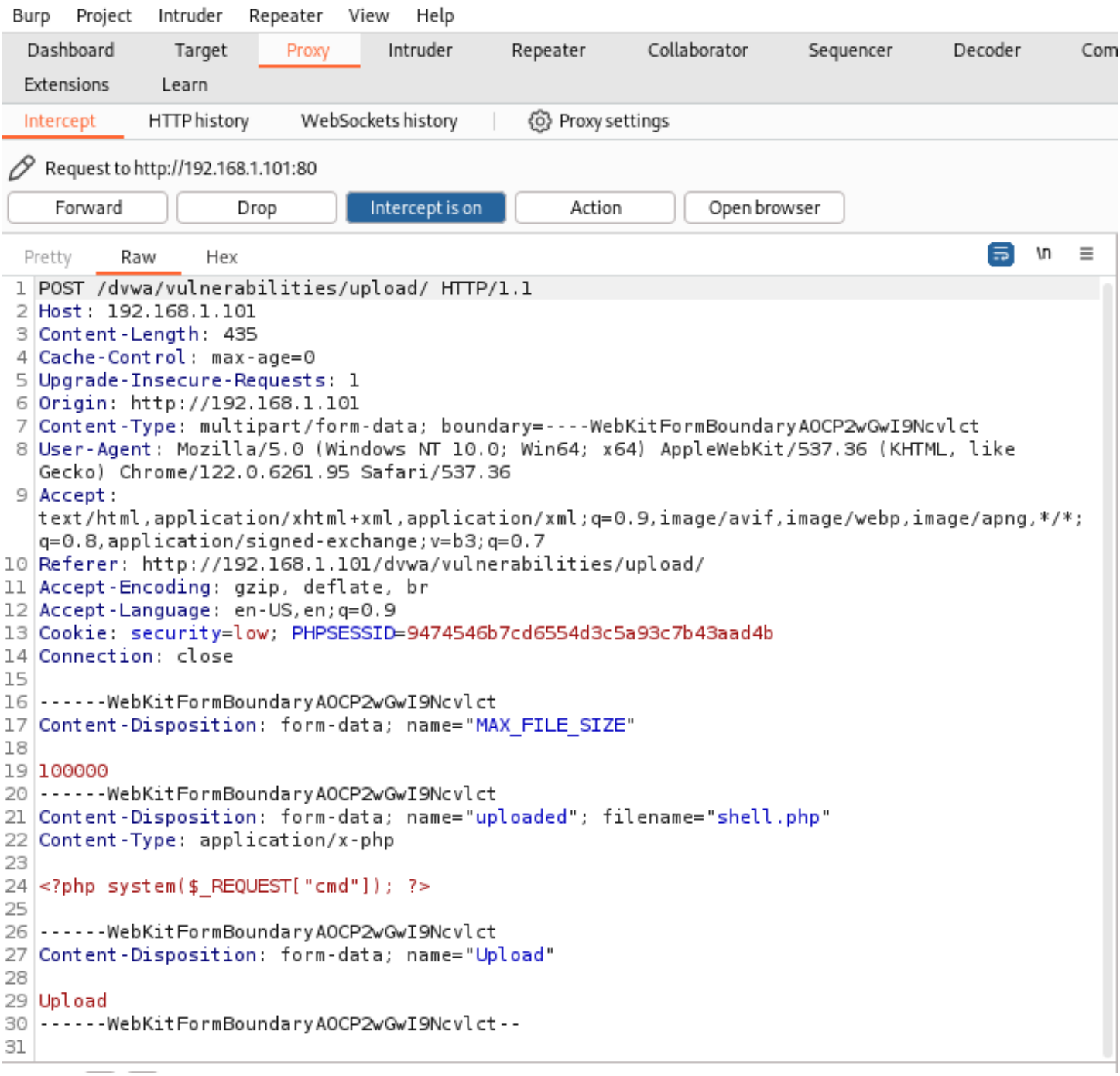
Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo **di intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite**.

1) Mi connetto dal browser alla macchina Metasploitable

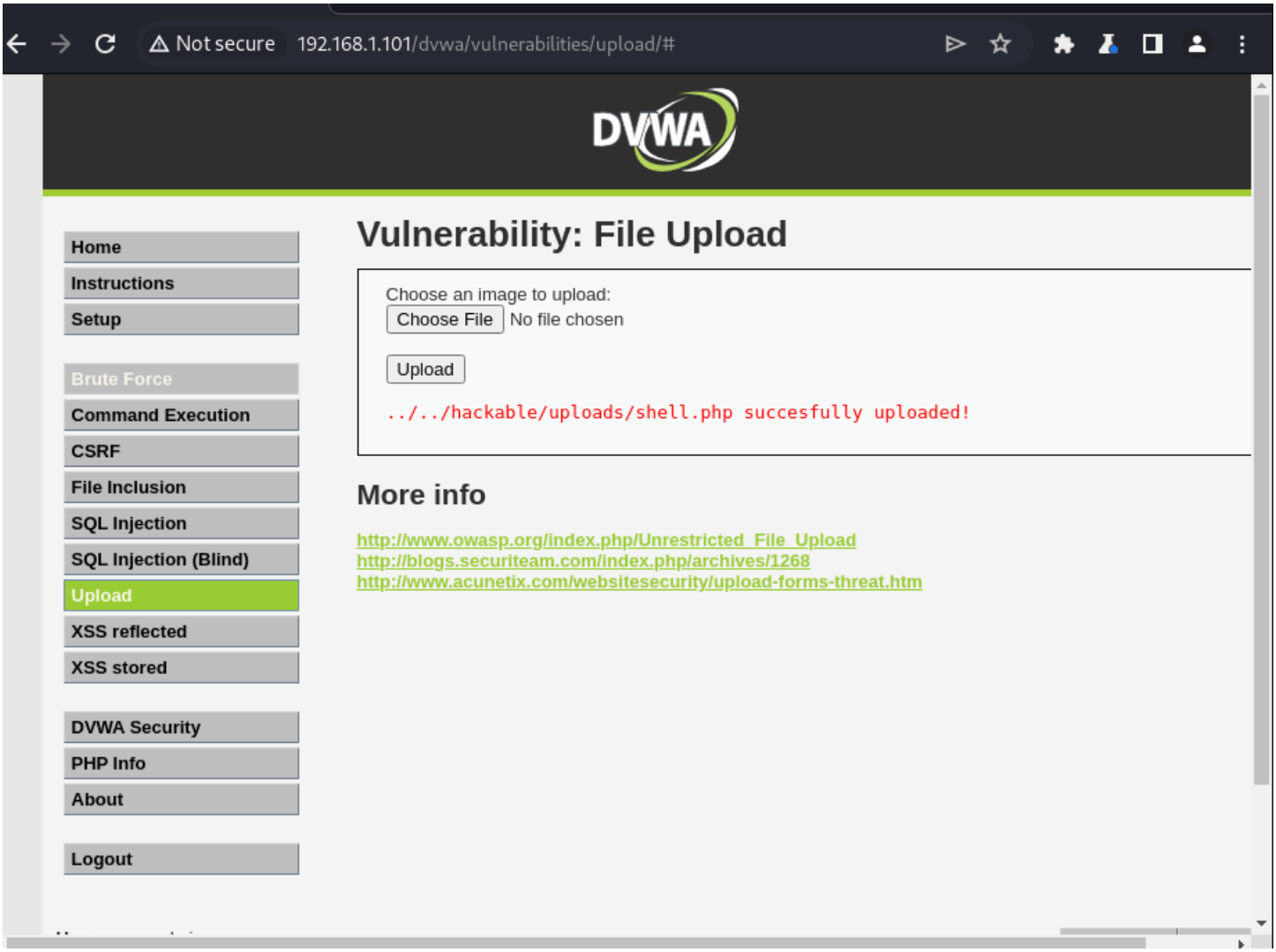


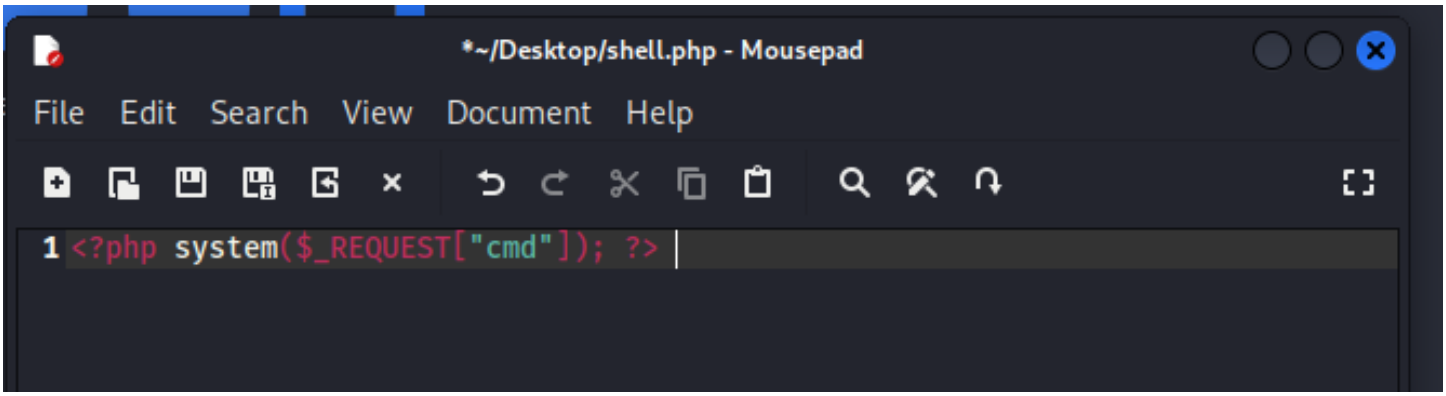
2) Mi sposto nella DVWA e faccio il login, nel mentre attivo il tool BurpSuite per analizzare le richieste


Damn Vulnerable Web Ap
Not secure
192.168.1.101/dvwa/login.php
DVWA
Username
Password
Login

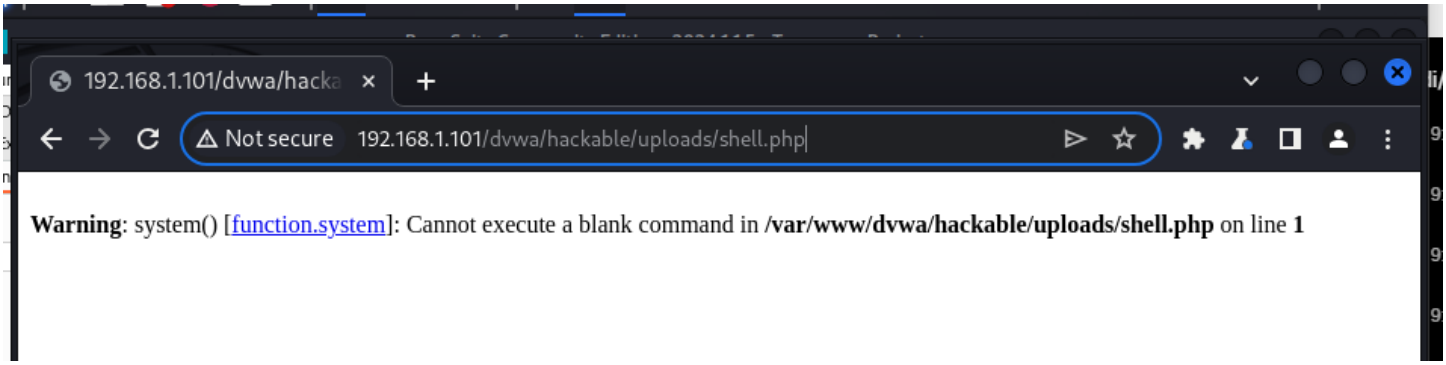


3) Di seguito mi sposto in Upload e carico la shell. (la shell l'ho creata su kali seguendo le istruzioni della traccia dell'esercizio)





4)Mi collego al path ma ricevo l'errore, perchè non abbiamo specificato nessun argomento.



5) Quindi aggiungo il parametro “cmd=ls” nella GET, ed infatti ci viene restituita la lista dei file. Possiamo vederlo anche da BurpSuite, che ci da anche la possibilità di modificare la richiesta prima di inviarla.