W13D1 Pratica

Giacomo di Giacinto

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.

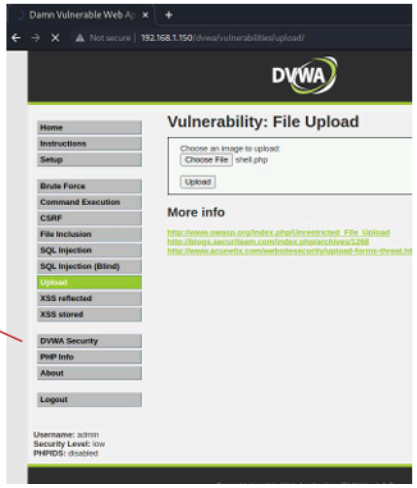
Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo **di intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite**.

Suggerimento:

Accedete alla DVWA dalla macchina Kali via browser, vi consigliamo di mantenere sempre aperta una sessione di BurpSuite per intercettare ogni richiesta e analizzare il contenuto.

Prima di iniziare configurate il «security level» della DVWA a «LOW» dalla scheda DVWA Security.

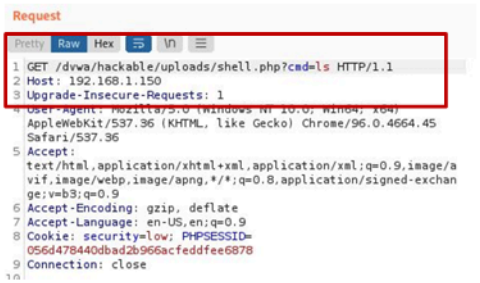
Successivamente spostatevi sulla scheda Upload per mettere in pratica il vostro exploit.



Suggerimento 2:

A destra un esempio di codice minimale della shell da caricare.

Una volta caricata la shell, essa accetta un parametro tramite richiesta GET nel campo cmd **(esempio della richiesta in figura nel rettangolo rosso). Guardate attentamente come viene passato il parametro cmd tramite la GET**



Potete trovare sul web shell molto più sofisticate, con interfaccia grafica e funzioni avanzate.

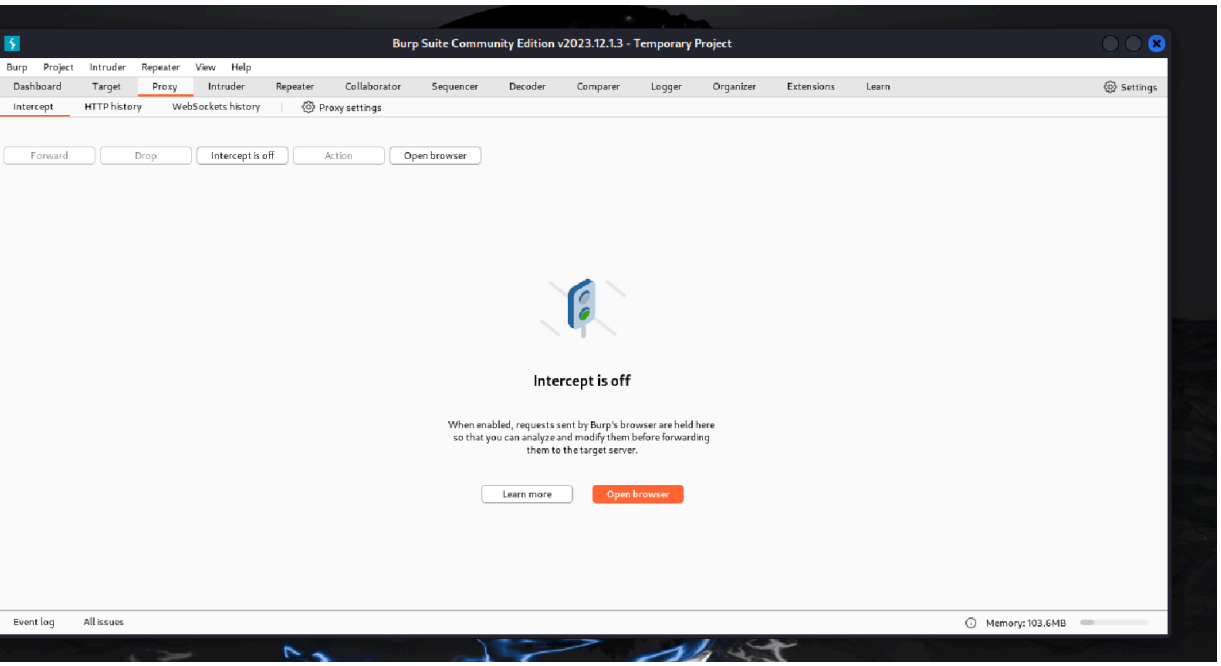
Lo studente che ha completato l'esercizio

Consegna:

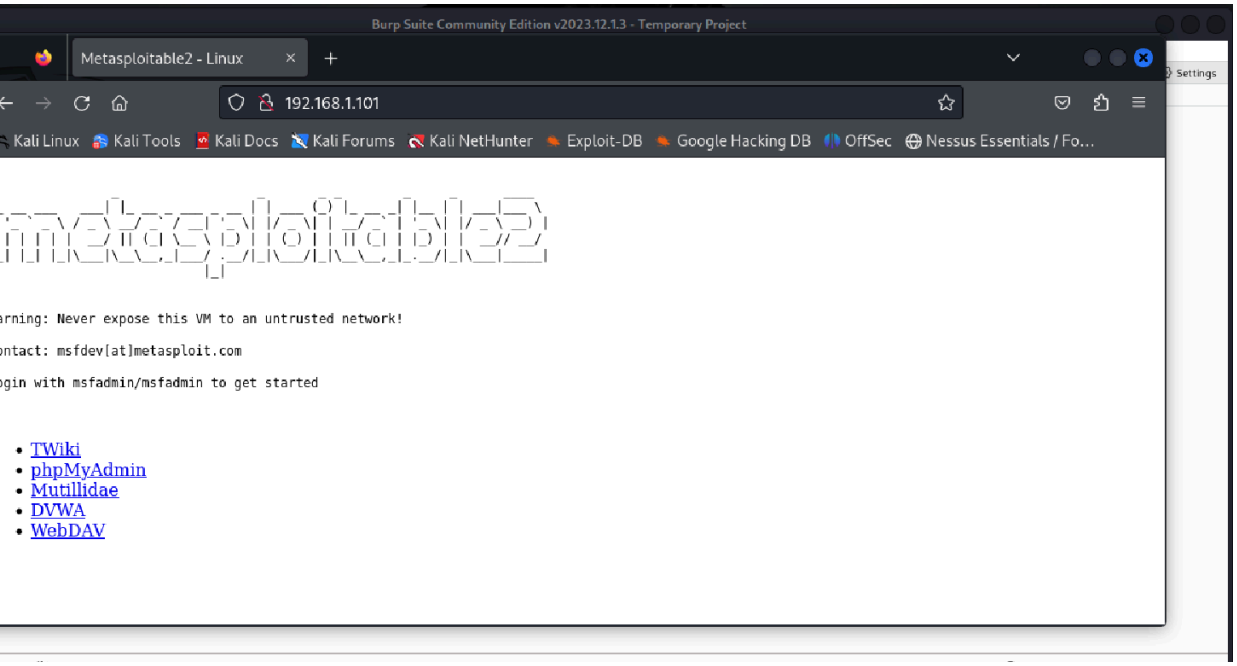
1. Codice php
2. Risultato del caricamento (screenshot del browser)
3. Intercettazioni (screenshot di burpsuite)
4. Risultato delle varie richieste
5. Eventuali altre scoperte della macchina interna
6. BONUS: usare una shell php più sofisticata

1ping macchine

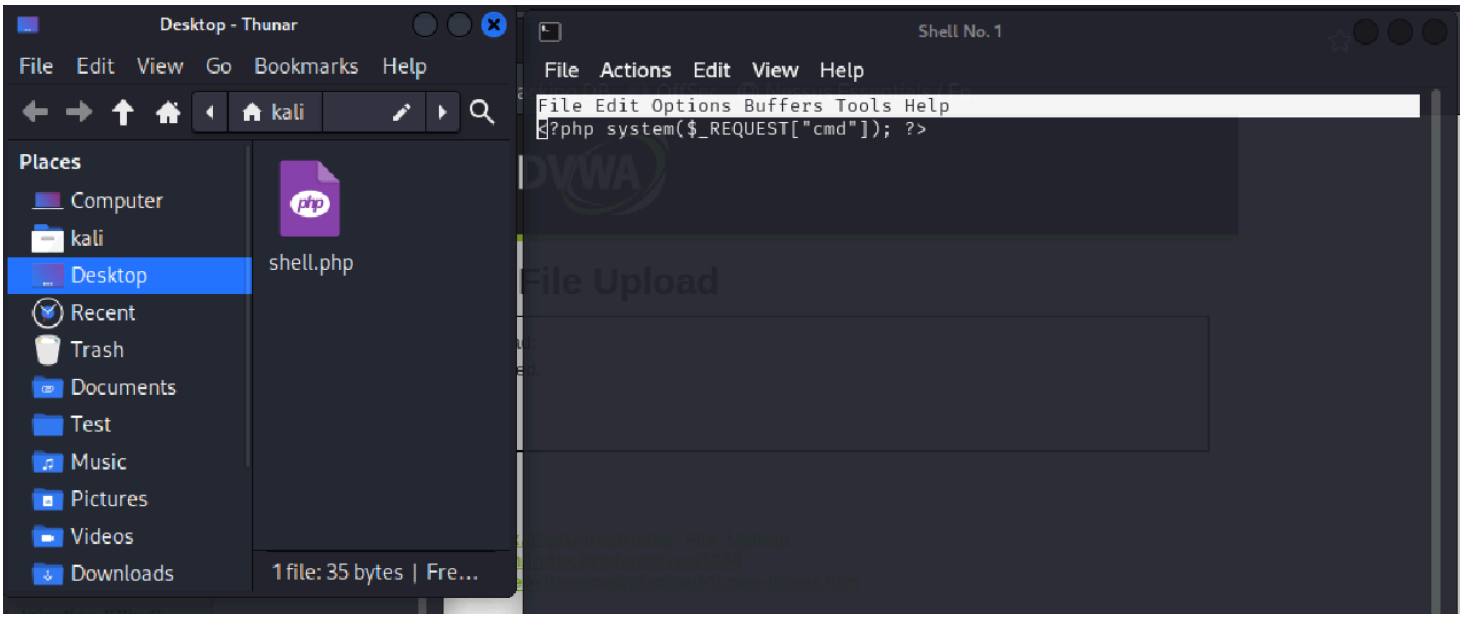
2aproburpsuite



3aprire la dvwa impostando sicurezza low

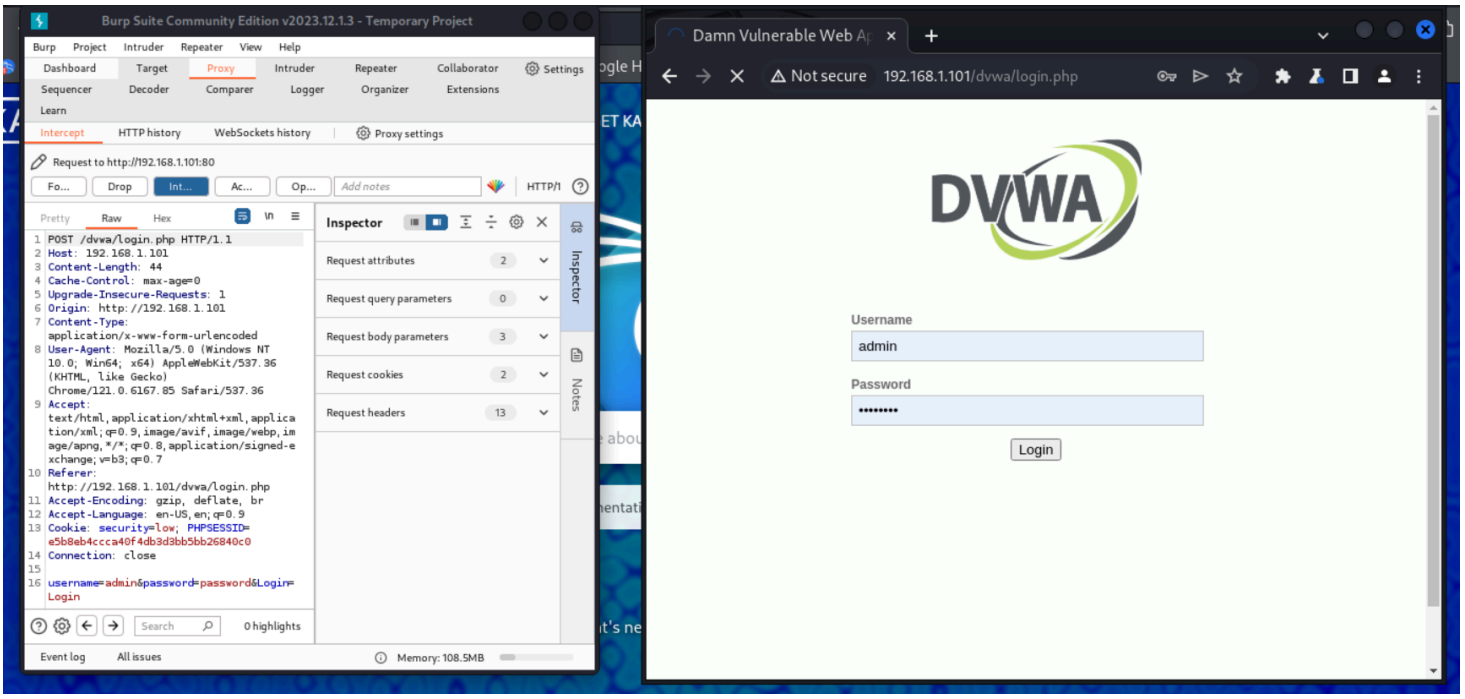


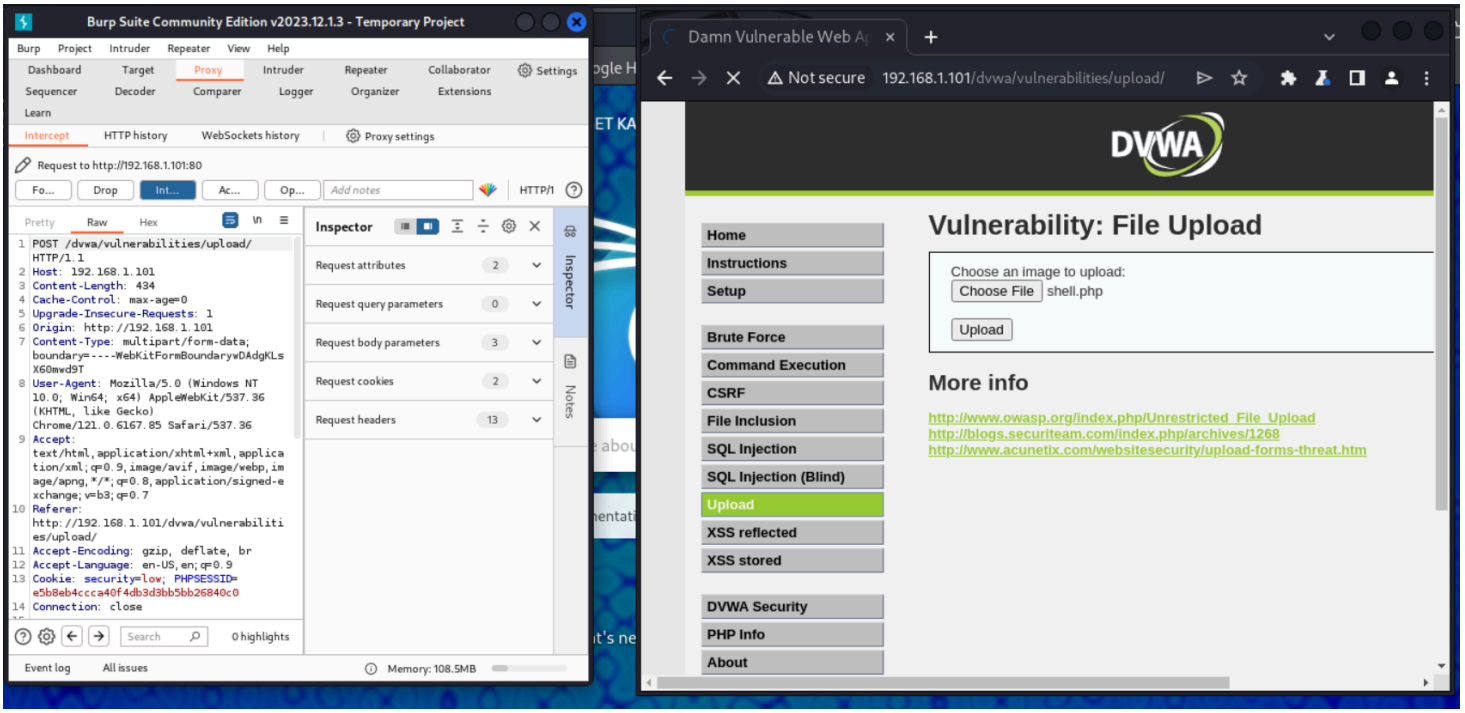
4 creare il file .php

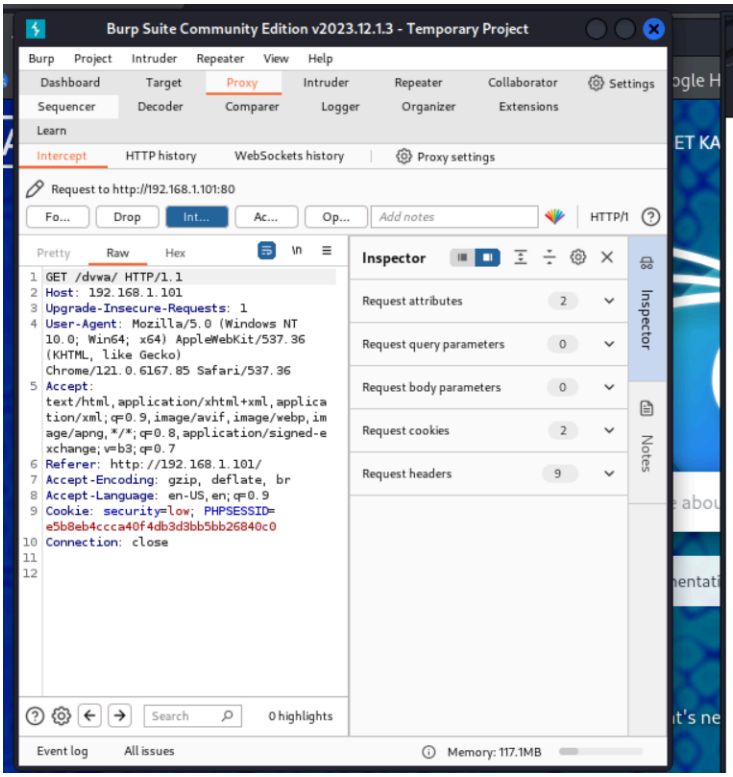


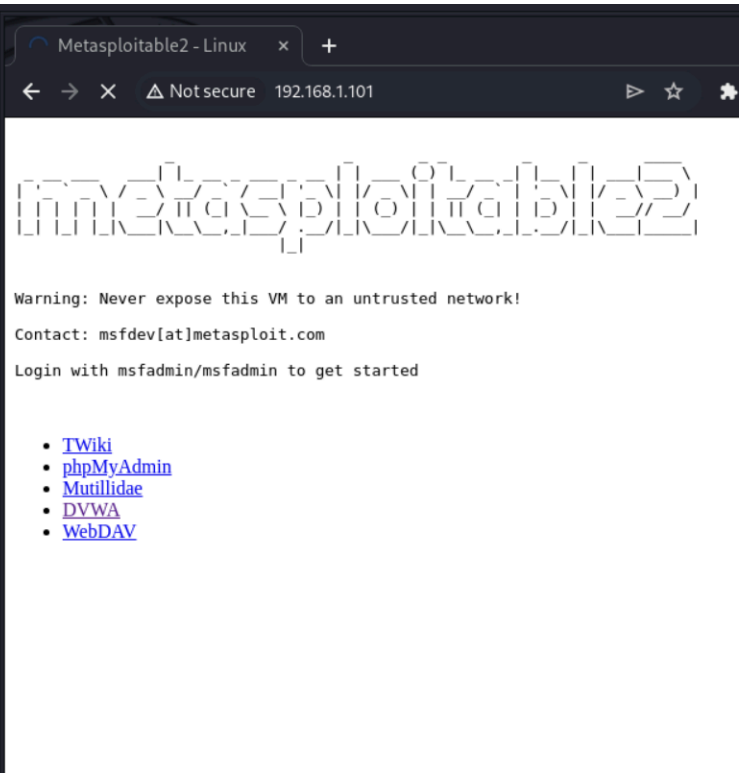
5)analizzo i diversi verbi a cosa corrispondono.

per una richiesta di visita di una pagina web il verbo è GET mentr quando andiamo ad inserire dei dati, sia come upload che come credenziali il verbo è POST






Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Settings
Sequencer Decoder Comparer Logger Organizer Extensions
Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.1.101:80
Fo... Drop Int... Ac... Op... Add notes HTTP/1
Pretty Raw Hex
1 GET /dvwa/ HTTP/1.1
2 Host: 192.168.1.101
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
5 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
6 Referer: http://192.168.1.101/
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Cookie: security=low; PHPSESSID=e5b8eb4ccca40f4db3d3bb5bb26840c0
10 Connection: close
11
12
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 2
Request headers 9
Inspector
Notes
Search 0 highlights
Event log All issues
Memory: 117.1MB


Metasploitable2 - Linux
Not secure 192.168.1.101
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
TWiki
phpMyAdmin
Mutillidae
DVWA
WebDAV

5 upload file .php