Report Esercizio 1 – SQL Injection su DVWA

| Titolo del Documento: | Report Attività di Laboratorio: Giorno 1 |

| Asset Sotto Analisi: | Macchina Virtuale Metasploitable |

| Indirizzo IP Target: | 192.168.13.150 |

| Indirizzo IP Attaccante: | 192.168.13.100 (Kali Linux) |

| Data dell'Attività: | 01 Settembre 2025 |

| Analisti: | [Landa Tracker S.P.A.] |

| Stato: | Completato |

TRACCIA GIORNO 1: SQL Injection su DVWA (Low e Medium)

Traccia Giorno 1:

Utilizzando le tecniche viste nelle lezione teoriche, sfruttare la vulnerabilità SQL injection presente sulla Web Application DVWA per recuperare **in chiaro** la password dell'utente **Pablo Picasso** (ricordatevi che una volta trovate le password, c'è bisogno di un ulteriore step per recuperare la password in chiaro)
NB: non usare tool automatici come sqlmap. È ammesso l'uso di repeater burp suite.

Bonus

- Replicare tutto a livello medium
- Recuperare informazioni vitali da altri db collegati
- Creare una guida illustrata per spiegare ad un utente medio come replicare questo attacco.

Requisiti

Requisiti laboratorio Giorno 1:

Livello difficoltà DVWA: LOW
IP Kali Linux: 192.168.13.100/24
IP Metasploitable: 192.168.13.150/24

1. **Livelli di Sicurezza** configurati in DVWA:

- **Low** per la prima parte.
- **Medium** per la seconda parte.

Assegnazione ip

```
└─$ sudo ip addr add 192.168.13.100/24 dev eth0
```

```
msfadmin@metasploitable:~$ sudo ip addr add 192.168.13.150/24 dev eth0
```

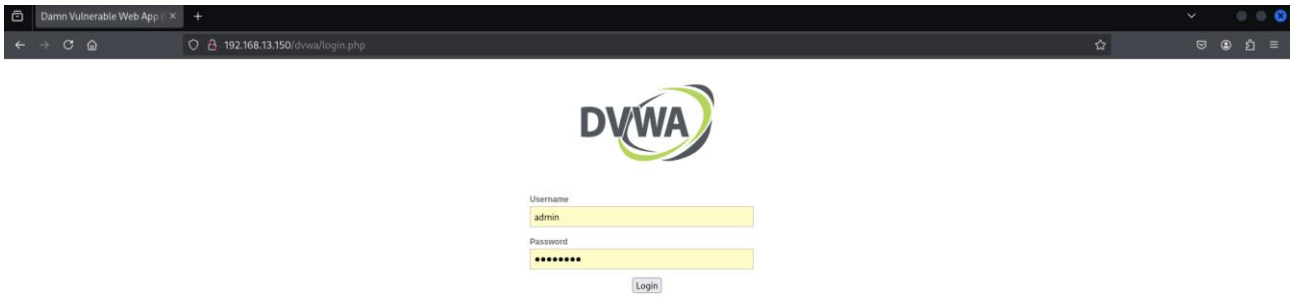
Controllo degli ip

```
inet 192.168.13.100/24 brd 192.168.13.255 scope global eth0
```

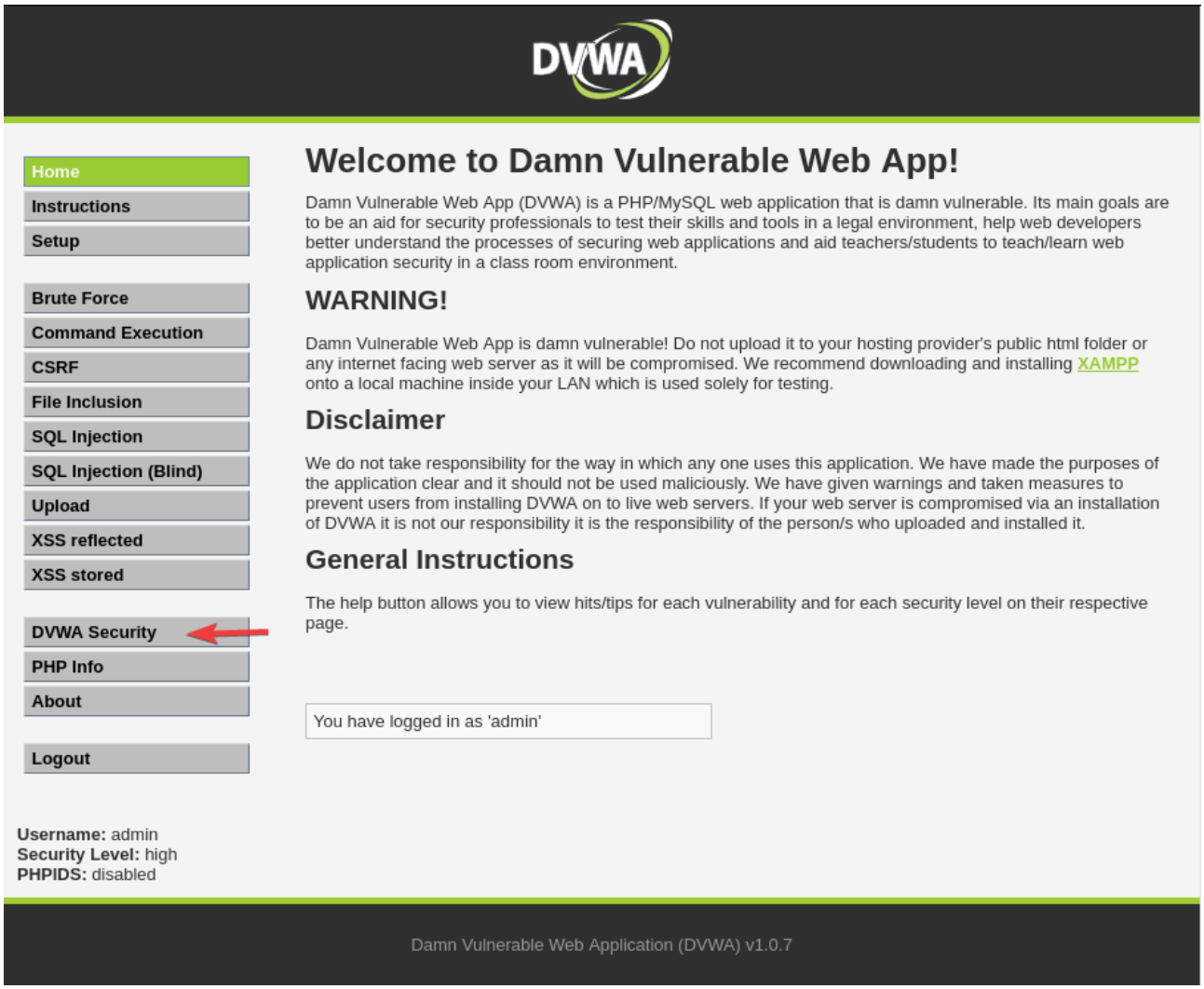
```
inet 192.168.13.150/24 scope global secondary eth0
```

Collegamento DVWA

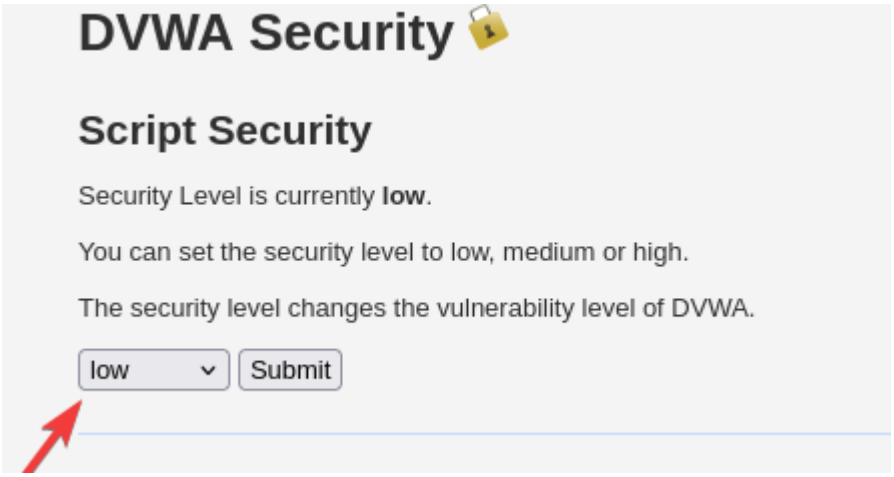
Ci colleghiamo all'URL http://192.168.13.150/dvwa e dopo aver inserito le credenziali **admin** e **password**.



Impostazioni di sicurezza



Una volta entrati su DVWA clicchiamo per entrare nel menù DVWA Security e impostiamo la sicurezza su **low**



Recupero delle credenziali con attacco SQL Injection

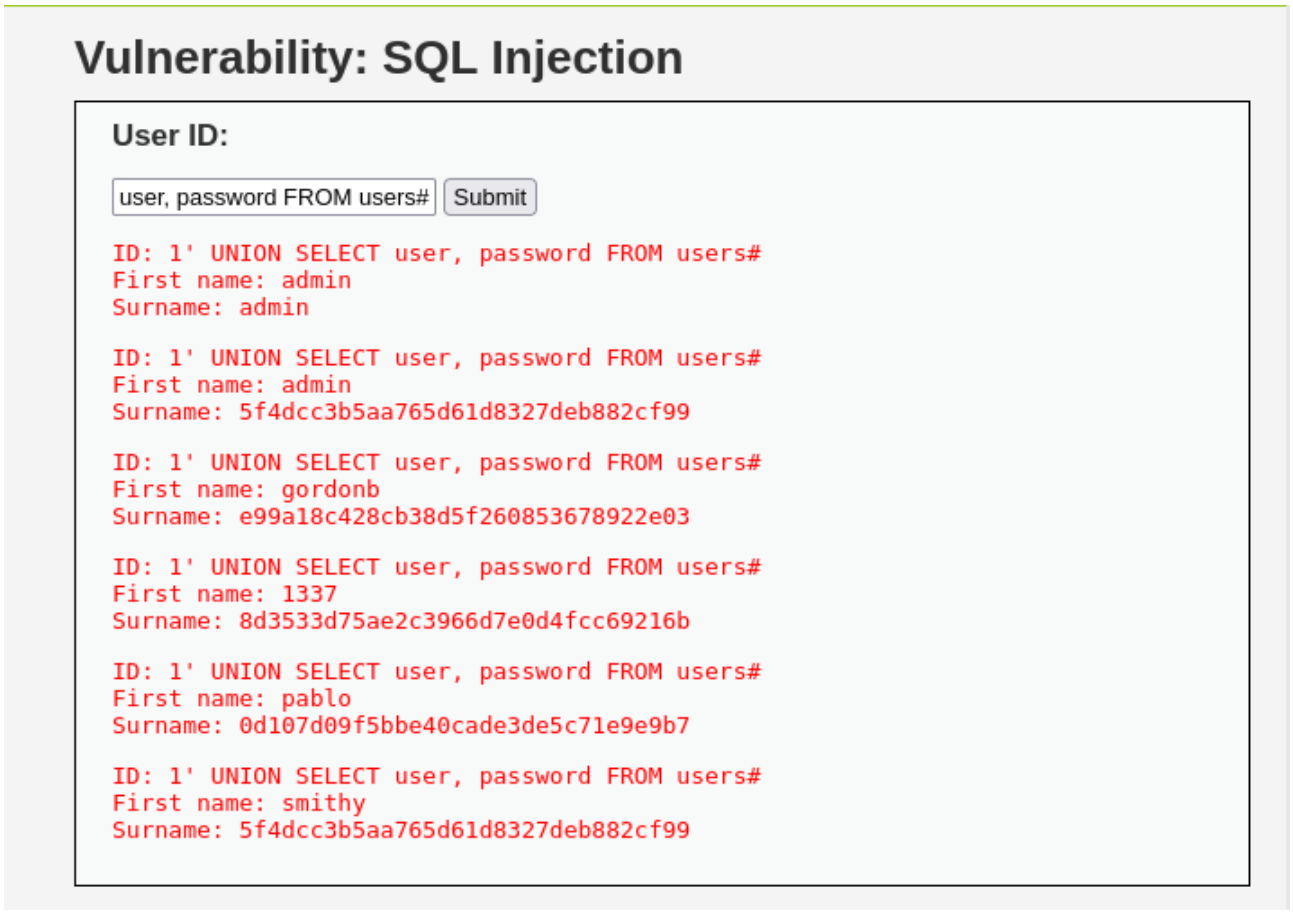
Entriamo nella sezione del menù “SQL Injection”

Scopriamo innanzitutto quali tabelle e colonne mi fornisce il database col comando

' UNION SELECT concat(TABLE_SCHEMA,".", TABLE_NAME), COLUMN_NAME FROM INFORMATION_SCHEMA.COLUMNS WHERE table_schema="dvwa" –

Inseriremo poi il seguente comando per ottenere una lista completa degli utenti MA con la password hashata e quindi ancora oscurata:

1' UNION SELECT user, password FROM users#



Isoliamo poi solo i dati dell'utente che a noi interessa, in questo caso "Pablo" col comando:
' UNION SELECT user, password FROM dvwa.users WHERE user='Pablo' –

Risultati ottenuti:

Nome utente: **Pablo**

Password hash: **0d107d09f5bbe40cade3de5c71e9e9b7**

Ottenere password hashate

L'hash **0d107d09f5bbe40cade3de5c71e9e9b7** possiamo ottenerlo in chiaro in due modi principali, utilizzando john the ripper o usando il sito https://crackstation.net, entrambi ci danno la conferma che la password equivale a letmein.

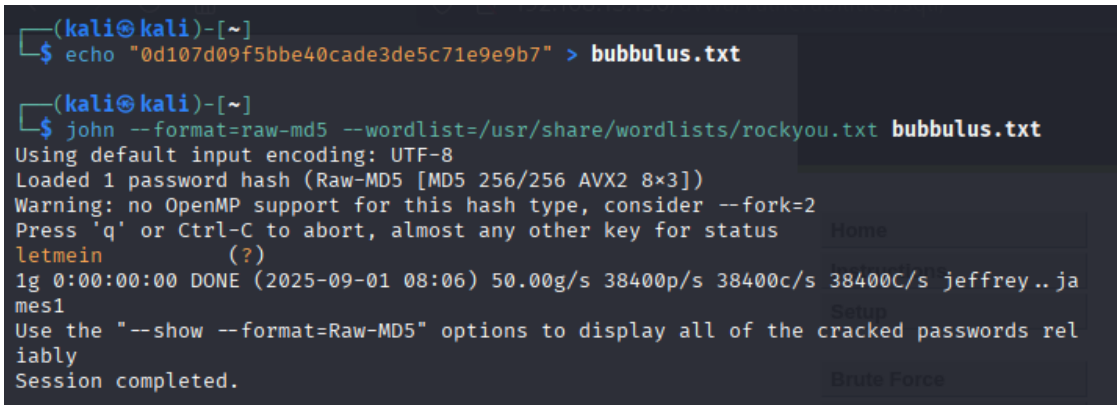
John The Ripper

Dopo aver salvato l'hash MD5 della password di Pablo in un file text chiamato "Bubbulus.txt" col comando:

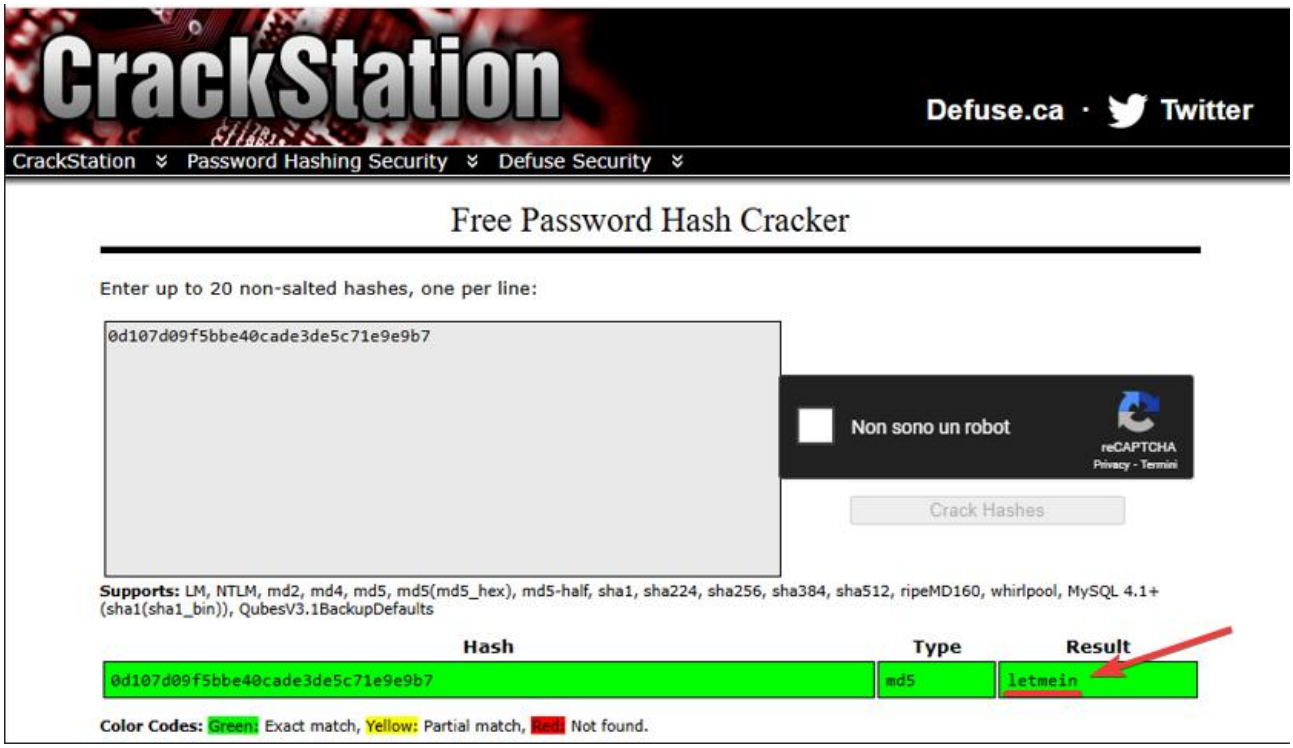
"echo "0d107d09f5bbe40cade3de5c71e9e9b7" > bubbulus.txt "

Utilizziamo poi il seguente comando per crackare la password:

john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt bubbulus.txt

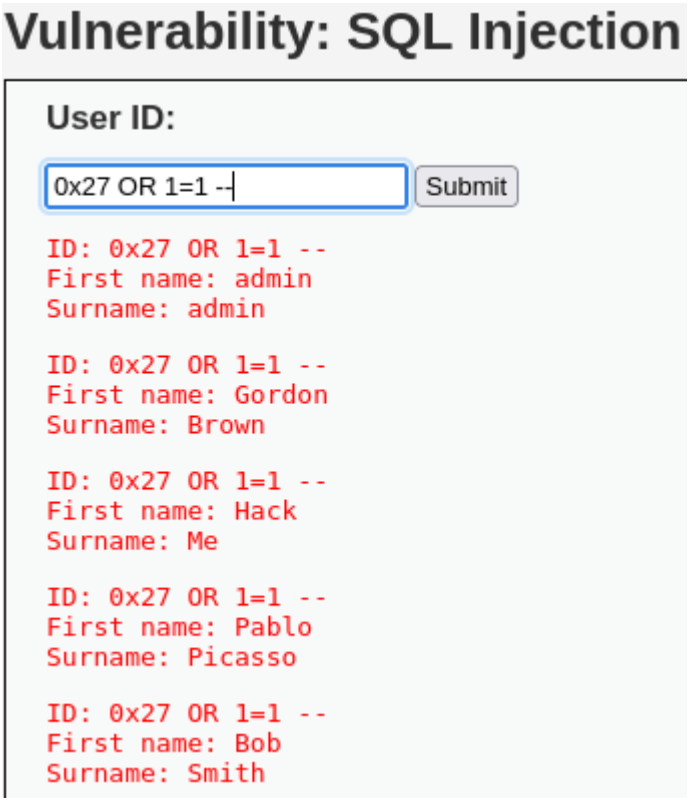


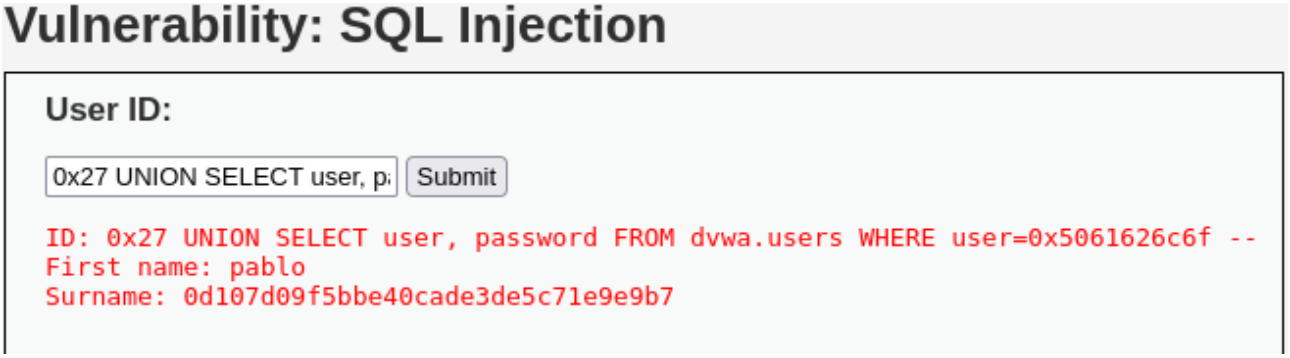
CrackStation



Una volta inserito l'hash crackstation ci darà in automatico il risultato della password che corrisponde con quella presa in precedenza.

SQL Injection con sicurezza Medium





Dopo aver impostato la sicurezza su medium seguendo i passaggi di prima abbiamo poi seguito gli stessi passaggi di prima ma usando il codice esadecimale per scrivere le cose.

0x27 è il formato hexadecimal per l'apostrofo (').

0x5061626c6f è il formato hexadecimal per Pablo.

La password viene poi decifrata con lo stesso procedimento utilizzato in precedenza.