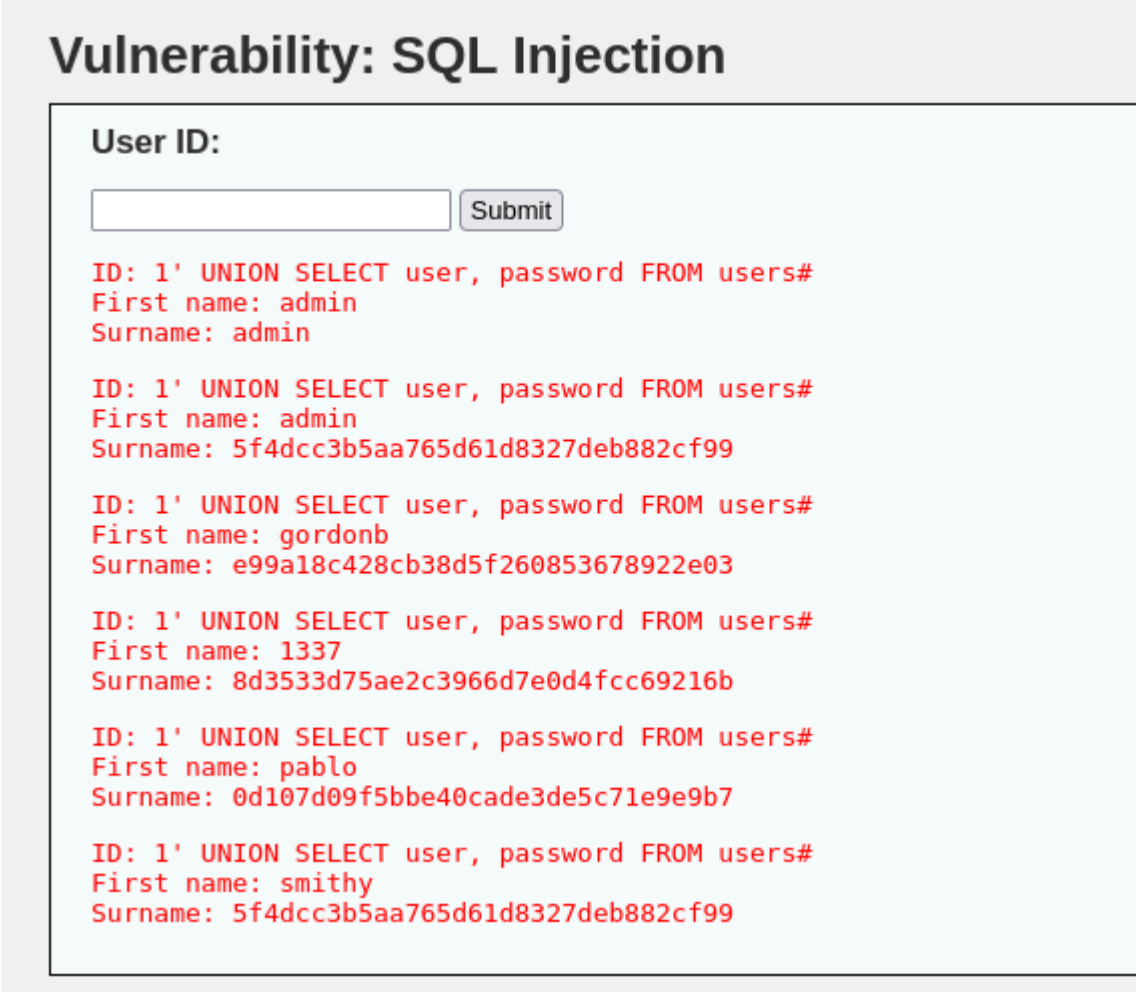
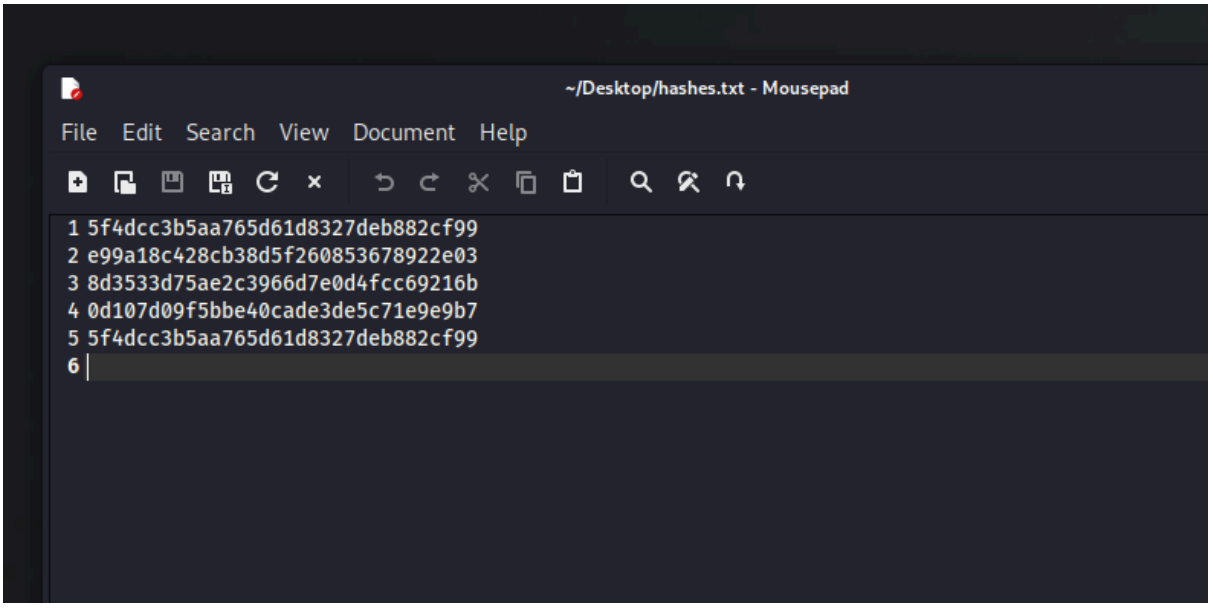
Esercizio S6L4 - John the Ripper e Cracking di Password

L’obiettivo di questo esercizio è comprendere le vulnerabilità presenti in un'applicazione web sfruttabile come DVWA, ospitata su Metasploitable. L’attività ci guida attraverso l’esecuzione di un attacco di SQL Injection per estrarre password hashate e successivamente usare strumenti di cracking per ottenere le password in chiaro. Questo processo evidenzia l'importanza della sicurezza dei database e ci aiuta a capire come proteggere meglio le applicazioni da attacchi comuni.

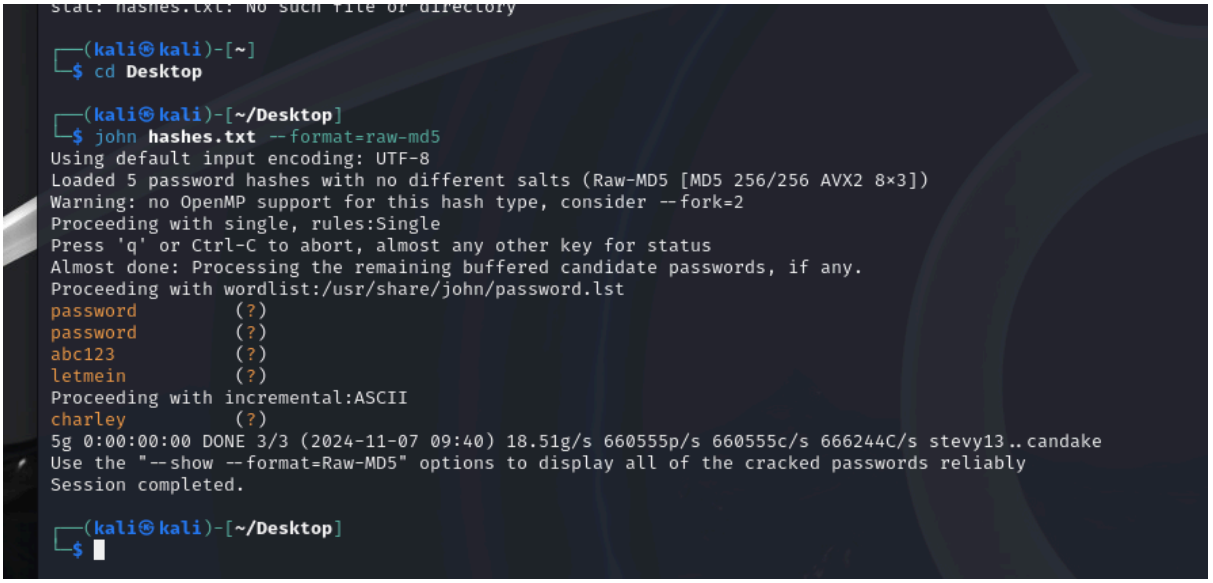
Per craccare le password, eseguiamo una SQL Injection per accedere ai dati riservati nel database della DVWA. Una volta ottenute le password hashate, le esportiamo in un file di testo per il cracking. Infine, utilizziamo John the Ripper, un potente strumento di cracking, per decriptare le hash e rivelare le password originali.



Il primo screenshot mostra il risultato della SQL Injection. Inserendo 1' UNION SELECT user, password FROM users#, siamo riusciti a ottenere i nomi utente e le password hashate dalla tabella users nel database di DVWA, come visibile nella GUI.



Il secondo screenshot illustra il file in cui abbiamo salvato le password hashate. Questo file serve come input per John the Ripper e permette di avviare il processo di cracking. Le hash sono salvate una per riga, pronte per essere analizzate dal nostro tool di cracking.



Il terzo screenshot mostra il risultato di John the Ripper. Dopo aver avviato il cracking delle hash, lo strumento ha decifrato con successo le password in chiaro. Questo dimostra la vulnerabilità delle hash MD5 quando non sono adeguatamente protette, rivelando le password originali.

In questo esercizio, abbiamo visto come un attaccante può sfruttare SQL Injection e strumenti di cracking per accedere a informazioni riservate. Questa esperienza rafforza l'importanza di implementare misure di sicurezza robuste per proteggere i dati sensibili.