Relazione sull'Esercizio di Cracking delle Password Hashate nella DVWA

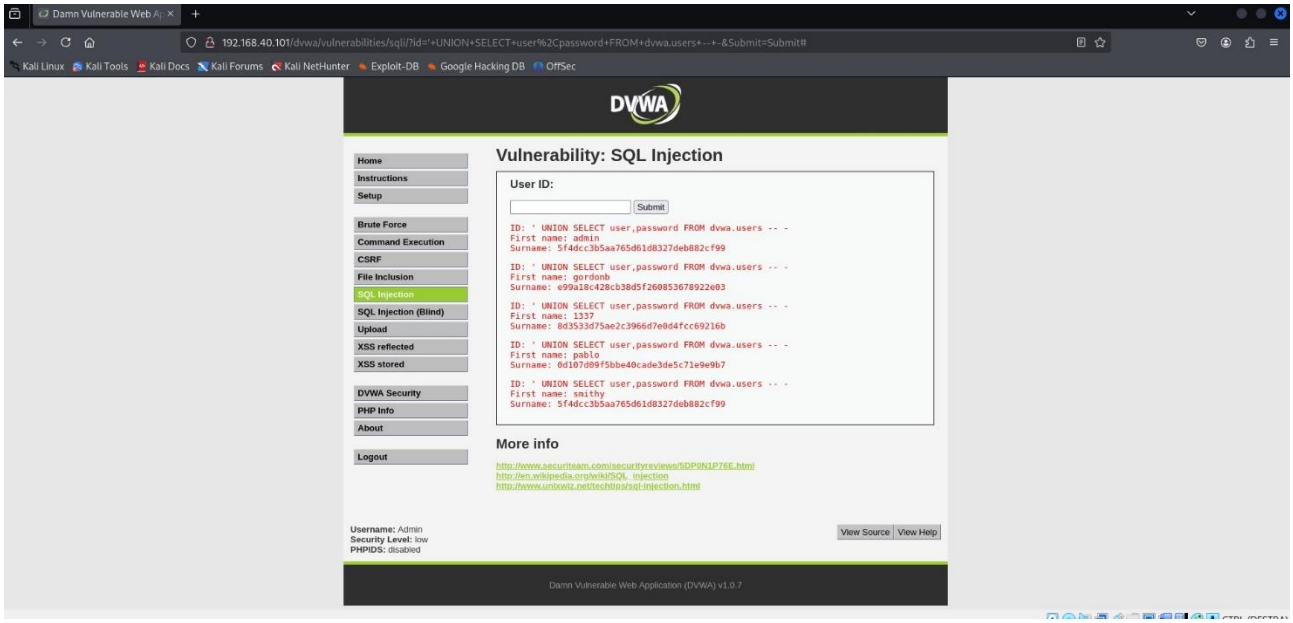
Introduzione

L'esercizio svolto aveva come obiettivo principale il recupero delle password hashate presenti nel database della **DVWA** (Damn Vulnerable Web Application) e la successiva decifrazione di queste password utilizzando strumenti di cracking come **John the Ripper**.

Impostazione dell'Ambiente

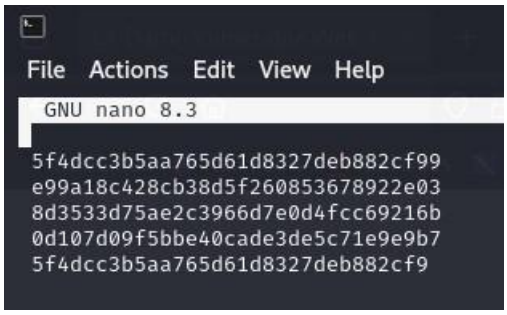
1. **Accesso alla DVWA**:
    - La DVWA è stata accessibile tramite la macchina virtuale **Metasploitable**, un ambiente appositamente configurato per test di sicurezza. Dopo aver effettuato il login, è stata selezionata la sezione **DVWA**.
    - Il **livello di sicurezza** della **DVWA** è stato modificato da **High** a **Low** per facilitare l'esecuzione dell'esercizio, rendendo l'applicazione più vulnerabile agli attacchi.

Esecuzione dell'Esercizio



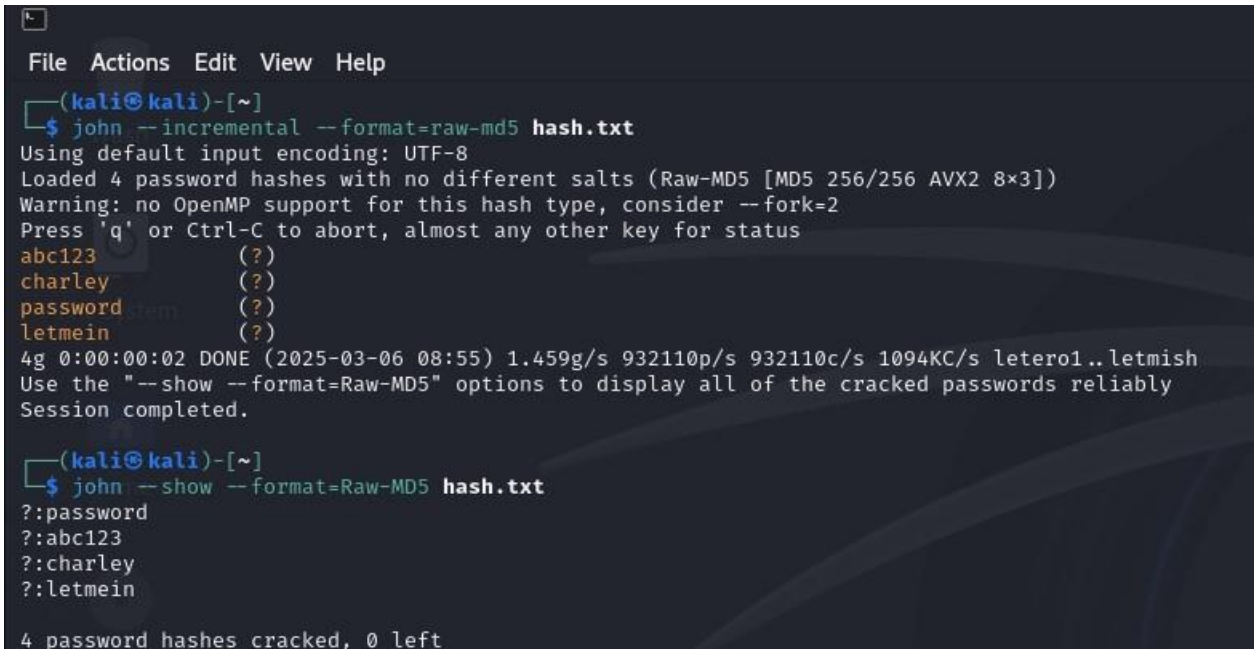
Nella sezione **SQL Injection** della DVWA, è stata inserita la seguente query: **' UNION SELECT user,password FROM dvwa.users -- -**

- Questa query ha permesso di estrarre dal database le informazioni relative agli utenti, comprese le password in formato hash.



Recupero delle Password Hashate:

- Dopo aver eseguito la query, sono stati ottenuti i dati degli utenti, tra cui le password hashate. Questi hash contenenti le password sono stati copiati e salvati in un file di testo sulla macchina virtuale **Kali Linux**

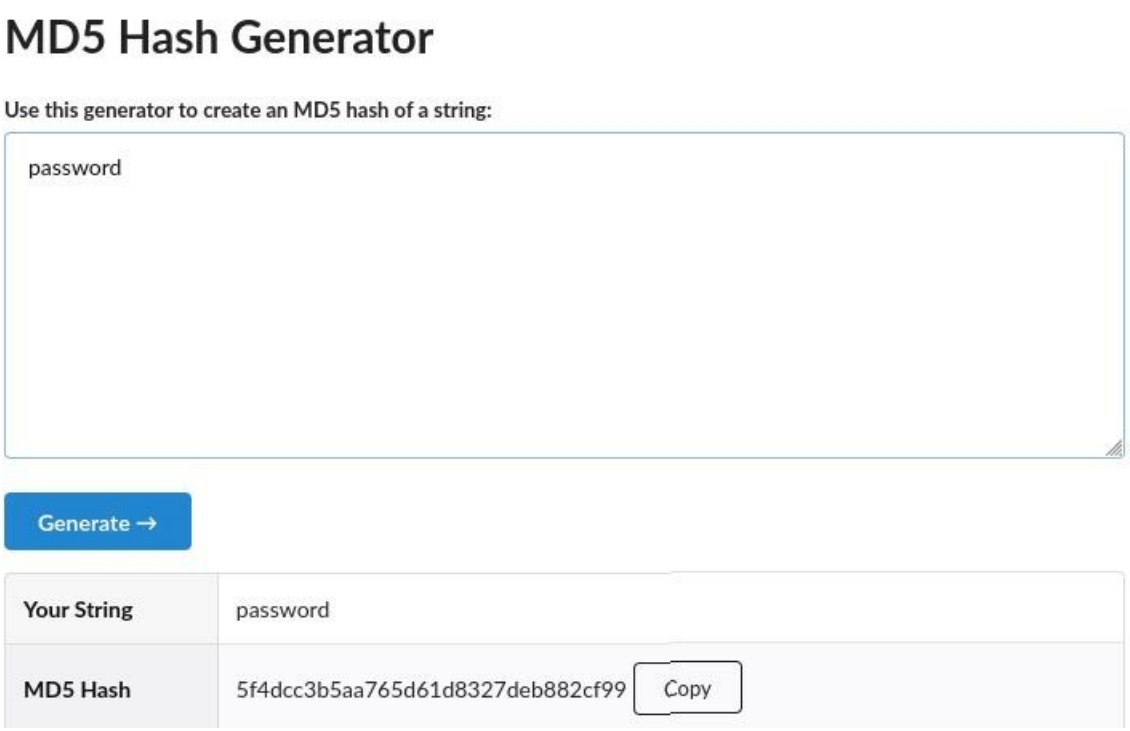


Cracking delle Password con John the Ripper:

Utilizzando il tool **John the Ripper**, è stato eseguito il comando: **john --incremental --format=raw-md5 hash.txt (file contenente gli hash delle password).**

- Il tool ha restituito le seguenti password in chiaro**: abc123, charley, password, letmein.**
- Per verificare le password decifrate, è stato utilizzato il comando**: john --show --format=Raw-MD5 hash.txt**

Verifica degli Hash con un Generatore MD5:



Per confermare la correttezza delle password decifrate, è stato utilizzato un generatore di hash MD5 online. Inserendo la parola **password**, è stato generato un hash che corrispondeva a quello presente nel database della DVWA, confermando così la validità del processo di cracking.

Conclusioni

L'esercizio mi ha permesso di comprendere l'importanza della sicurezza delle password e di testare la vulnerabilità di un sistema attraverso tecniche di SQL Injection e cracking delle password.