

John the Ripper

Esercizio Password cracking

Argomento:

Password Cracking – Recupero delle Password in Chiaro

Obiettivo dell'Esercizio:

Recuperare le password hashate nel database della DVWA e eseguire sessioni di cracking per recuperare la loro versione in chiaro utilizzando i tool studiati nella lezione teorica.

Istruzioni per l'Esercizio:

Recupero delle Password dal Database:

- Accedete al database della DVWA per estrarre le password hashate.
- Assicuratevi di avere accesso alle tabelle del database che contengono le password.

Identificazione delle Password Hashate:

- Verificate che le password recuperate siano hash di tipo MD5.

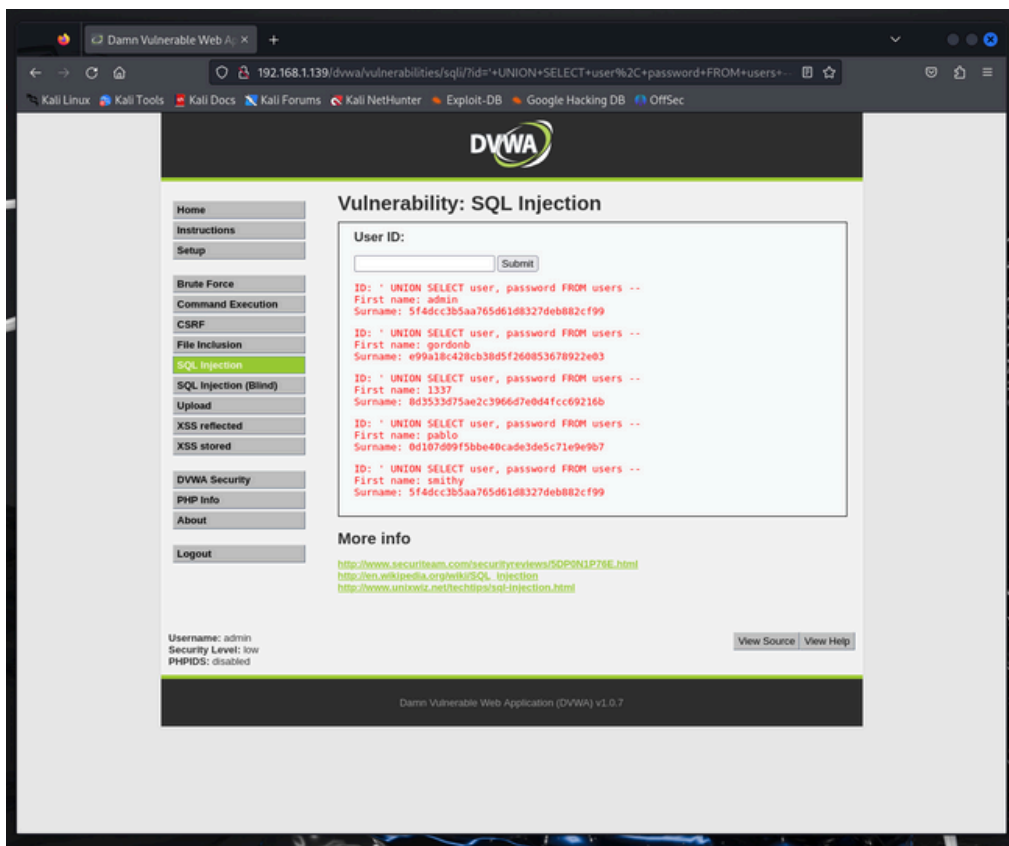
Esecuzione del Cracking delle Password:

- Utilizzate uno o più tool per craccare le password:
- Configurare i tool scelti e avviate le sessioni di cracking.

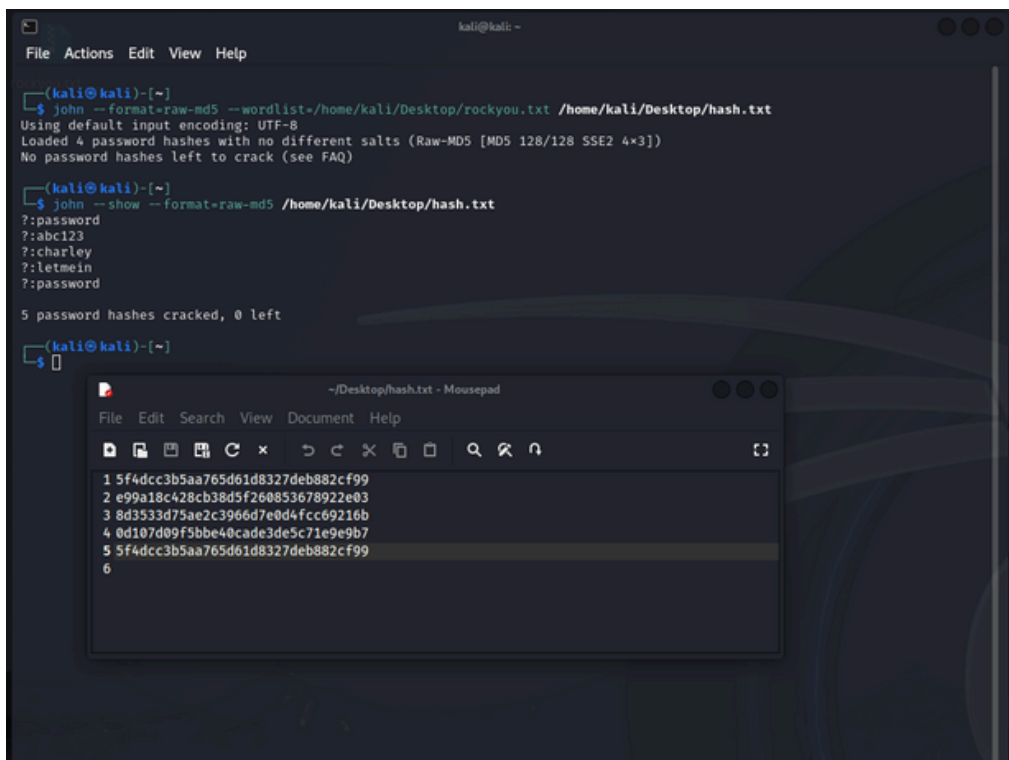
Obiettivo:

- Craccare tutte le password recuperate dal database.

Recupero hash md5 dvwa



Crack delle password



Relazione

Sono entrato nella DVWA, ho impostato la sicurezza su low e ho recuperato gli hash tramite SQL Injection. Successivamente, ho chiesto a ChatGPT di fornirmi i comandi da utilizzare con John the Ripper (JTR). Ho specificato che avevo creato la cartella hash.txt sul Desktop, e ChatGPT mi ha fornito sia il comando per craccare le password che il comando per visualizzarle con --show.

Lo scopo dell'esercizio era imparare come eseguire il cracking delle password con John the Ripper. Per l'esecuzione dell'esercizio è stato utilizzato il dizionario rockyou.txt.

Daniel_Gabriel_Costeanu