S6/L4

Traccia:

Utilizzando l’attacco SQL Injection (non blind), andare a compromettere il database di DVWA.

Bonus: Noterete che le password sono in codice hash. Trovare il modo per rendere le password in chiaro.

Per prima cosa, ci colleghiamo tramite la nostra macchina kali, alla DVWA con l’IP di metasploitable2. Dopo aver impostato il livello di sicurezza a “low” andiamo su SQL injection.

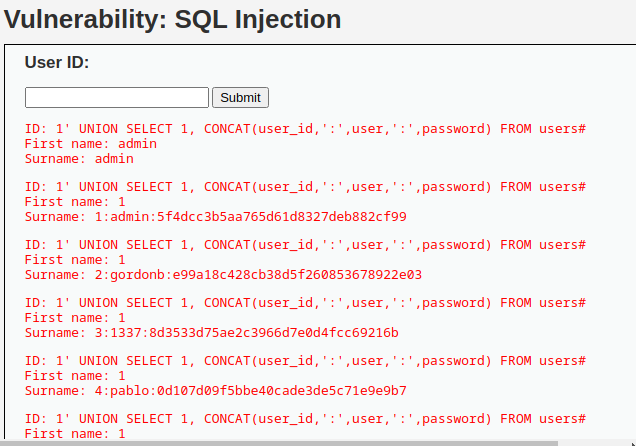
Un SQL injection è una forma di attacco informatico in cui un attaccante inserisce del codice SQL (malevolo) in un sito web. L'obiettivo principale è sfruttare le vulnerabilità di sicurezza nelle query SQL per ottenere accesso non autorizzato ai dati del database.

Al suo interno scriviamo una query del tipo:

1’ UNION SELECT 1, CONCAT(user\_id, ‘:’,user,’:’,password) FROM users#

L'obiettivo di questa query è estrarre informazioni riservate dalla tabella degli utenti del database.

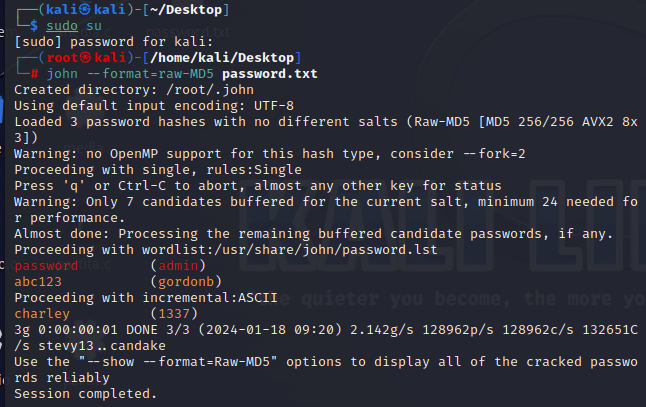
Viene inserita una nuova query che restituisce i risultati combinati con la query originale, l'obiettivo è ottenere informazioni sulla struttura della tabella users e recuperare i valori delle colonne: user\_id, user e password per ogni record nella tabella.



Convalidata la sua vulnerabilità, possiamo vedere che ci viene data una lista di nomi utenti e password non in chiaro, bensì in codice HASH, per vederle in chiaro abbiamo due opzioni:

* Copiare direttamente la riga di password criptata su uno dei tanti siti open source sul web (es. MD5 Center)
* Oppure creare un file di testo.txt su kali, inserendo le password in codice hash, dopo di che, da terminale e riga di comando usiamo “john the ripper” ovvero un software libero usato per il cracking delle passwords.

Usiamo il comando: John --format=raw-MD5 (questa opzione indica il formato delle password MD5) seguito dal file che abbiamo creato per eseguire un attacco brute force sulle password:



Ora possiamo vedere le password in chiaro per i relativi user.