REPORT

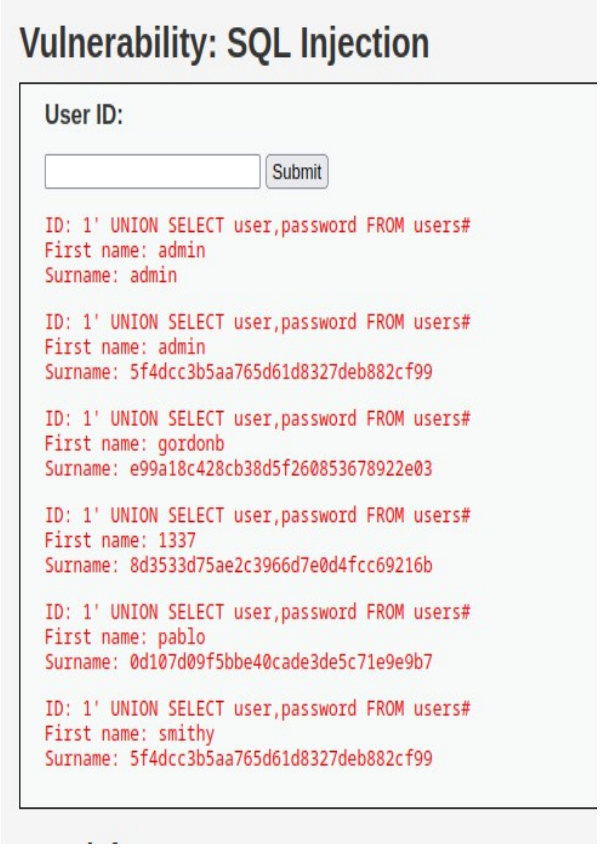
Spiegazione programma di cracking "John the Ripper"

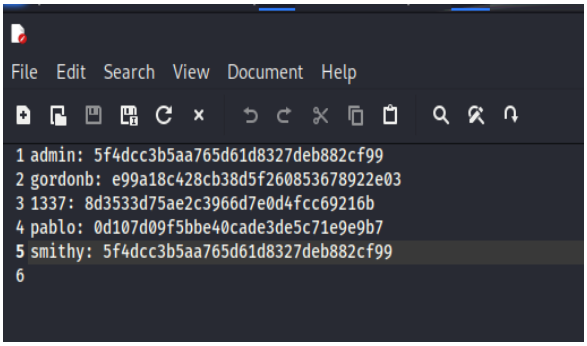
John the Ripper è un potente programma per "crackare" le password, che si utilizza in due tipi di cracking: forza bruta e attacco a dizionario.

- Nel cracking forza bruta, John the Ripper prova tutte le possibili combinazioni di caratteri fino a trovare la password corretta. È un processo che richiede tempo e molta potenza di calcolo, perché il programma deve provare diverse password possibili. Utilizza algoritmi di hashing per confrontare le password con l'hash della password crittografata, e se trova una corrispondenza, significa che ha trovato la password corretta.
- Nell'attacco a dizionario, John the Ripper utilizza una lista predefinita di parole o frasi comuni, ovvero un dizionario. Confronta queste parole o frasi con l'hash delle password crittografate per trovare una corrispondenza. Questo tipo di attacco sfrutta il fatto che molte persone utilizzano password deboli o facili da indovinare, come parole comuni o sequenze di tasti semplici.

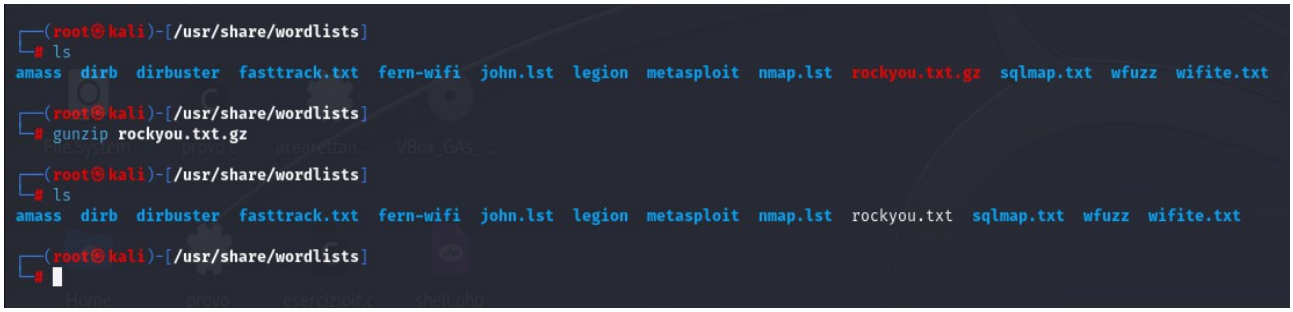
Cracking password con John the Ripper

Ho ottenuto gli utenti e le password criptate da un database sfruttando un attacco di SQL injection su DVWA. Questo mi ha permesso di estrarre le informazioni necessarie per il crack delle password, inclusi gli hash crittografati delle password degli utenti.

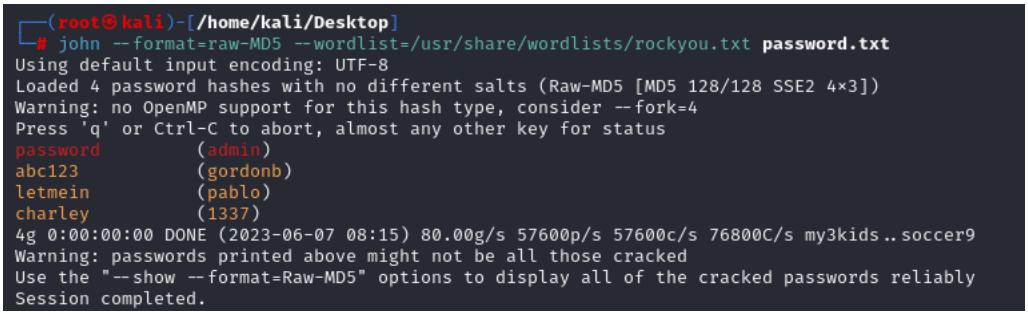




Ho estratto la lista delle password "rockyou.txt", che contiene password comuni e facilmente indovinabili. Ho utilizzato questa lista come input per John the Ripper, al fine di cercare corrispondenze tra gli hash crittografati delle password ottenute e le password presenti nella lista.



Ho lanciato John the Ripper con gli hash delle password ottenute e la lista delle password "rockyou". Il programma ha utilizzato algoritmi di hashing per confrontare gli hash crittografati delle password con quelle presenti nella lista. Quando ha trovato una corrispondenza, ha restituito la password in chiaro.



Risultati: John the Ripper è riuscito a trovare la maggior parte delle password corrispondenti agli hash crittografati, rivelando così le password in chiaro degli utenti. Tuttavia, ho riscontrato un problema nel programma: quando più utenti condividevano la stessa password, John the Ripper considerava solo la prima occorrenza della password duplicata e non rilevava quelle successive.

Cracking con Hashcat

Ho utilizzato Hashcat per decifrare le password crittografate utilizzando un attacco a dizionario. Ho utilizzato la stessa wordlist utilizzata con John the Ripper.

Ho avviato Hashcat con i seguenti parametri:

- Tipo di hash: MD5 con lo switch "-m"
- Tipo di attacco: Dizionario con lo switch "-a"