Traccia

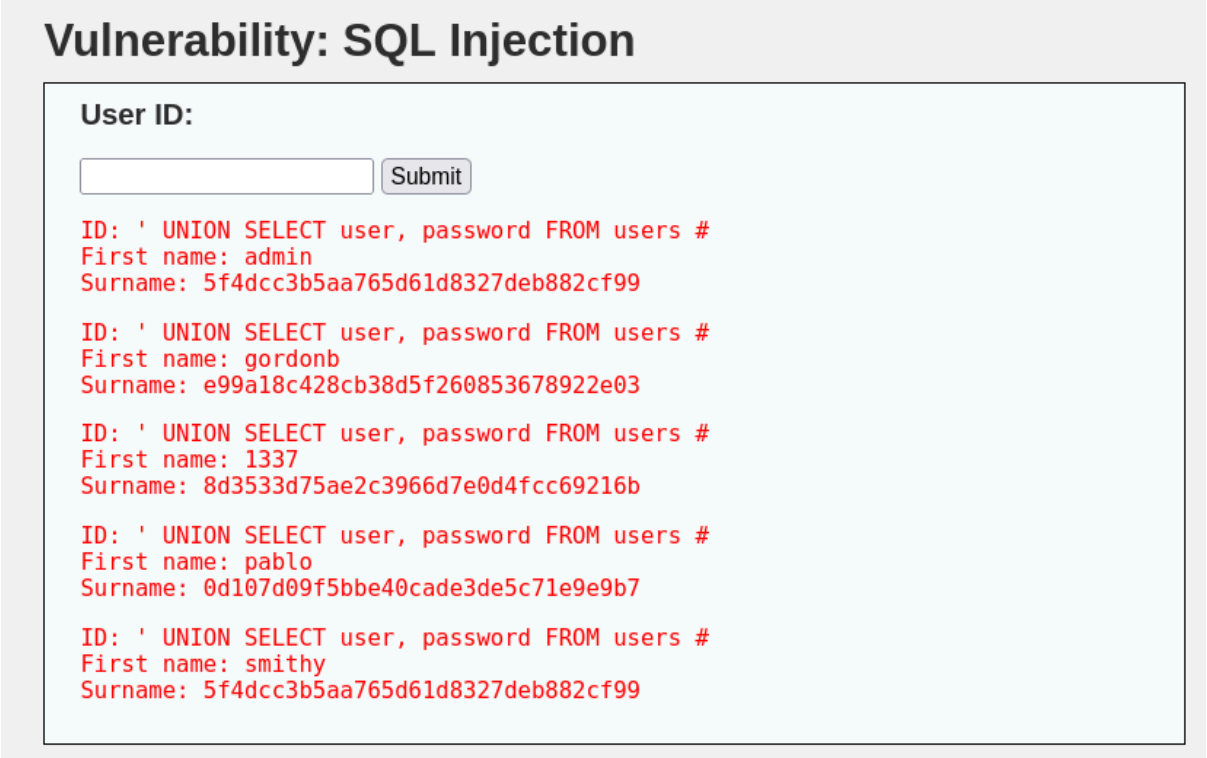
Recuperare le password dal DB della DVWA e provare ad eseguire delle sessioni di cracking sulla password per recuperare la versione in chiaro.

Svolgimento

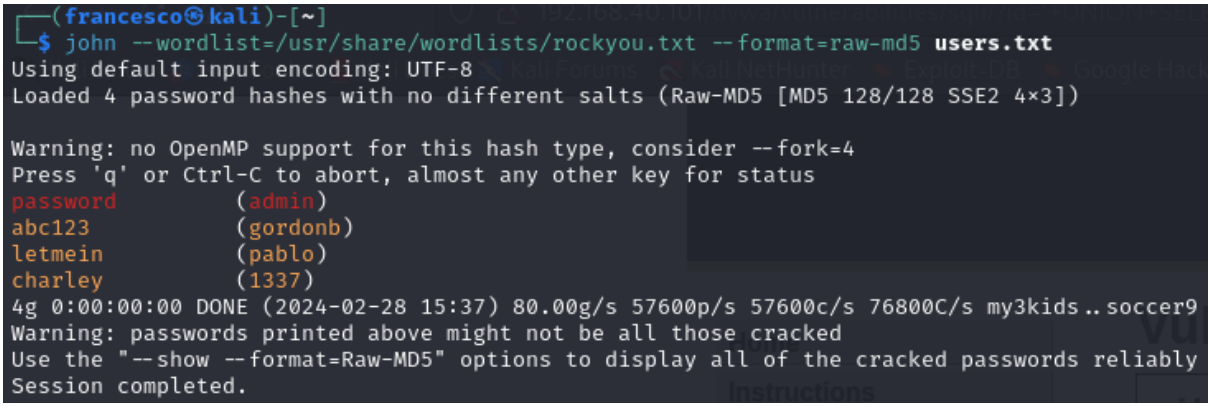
Per prima cosa si deve eseguire un attacco di tipo SQL injection, così da ottenere le password hashate. Il codice utilizzato è il seguente.

```
1' UNION SELECT user, password FROM users #
```

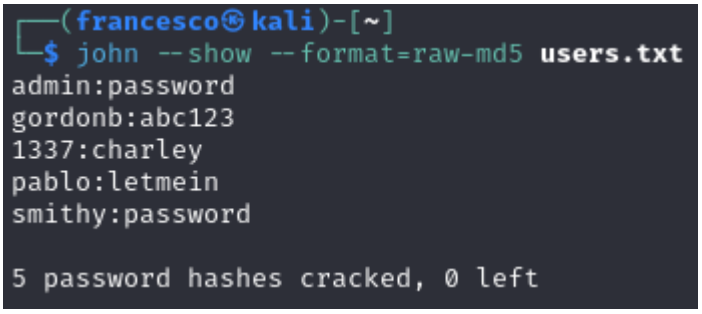
Si ottiene la seguente risposta.



Questa combinazione di user e password, deve essere inserita in un file txt, che dovrà essere passato come parametro a John the Ripper. JtR è un tool per il cracking delle password. Il comando da eseguire è il seguente.



Lo switch *–wordlist*, seguito da un file contenente delle password comuni, serve per eseguire un attacco di tipo dizionario.
Lo switch *–format*, serve per indicare in quale formato sono crittografate le password, se non si ha questa informazione, si deve provare finché non si trova il metodo corretto.
Il risultato del comando è una lista delle password trovate per ogni utente. Questa lista però, non è completa. Se si vuole la lista completa, bisogna eseguire il comando seguente.



Con questo comando JtR controlla le password salvate nel nostro file e le confronta con le password che ha decifrate, che sono salvate nel percorso *./john/john.pot*.