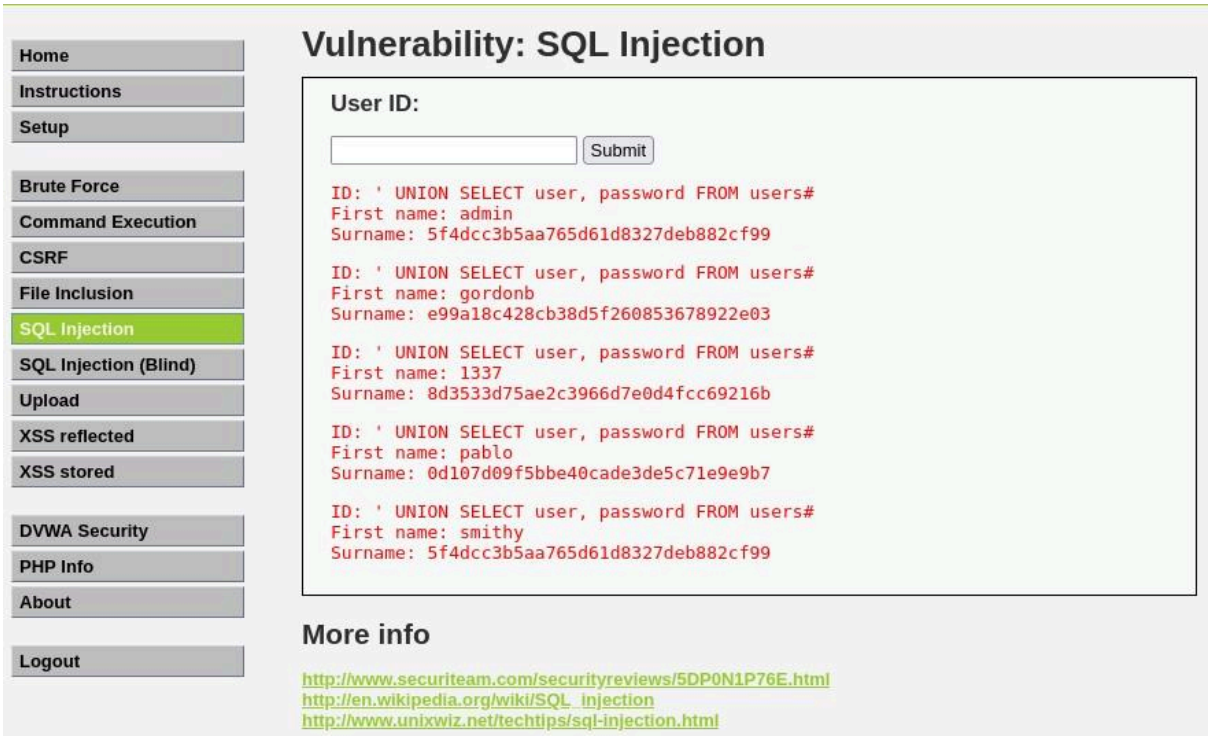
# CRACKING PASSWORD

Il lavoro da svolgere prevede di decriptare gli hash delle password che abbiamo trovato nella SQL injection di DVWA.
Il tool di cracking utilizzato è '**John The Ripper**'
La traccia è la seguente:

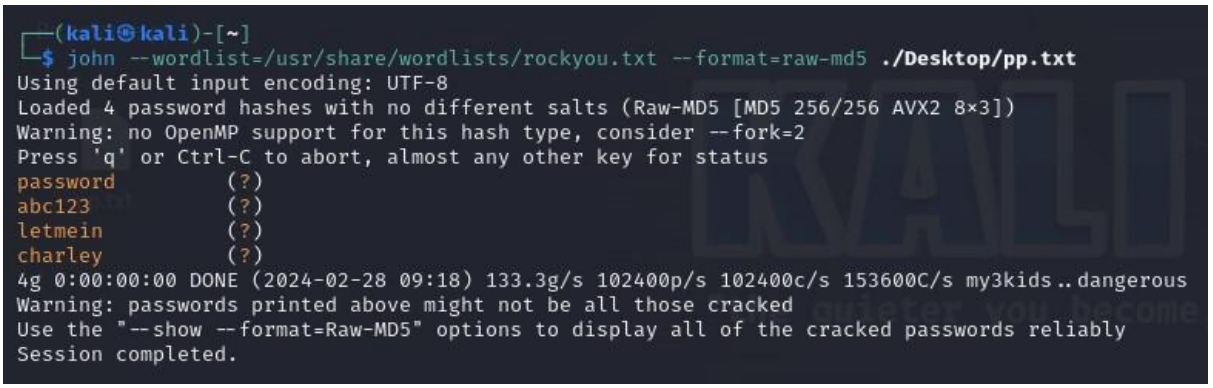
Se guardiamo meglio le password, della lezione precedente, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5. Recuperate le password dal DB e provate ad eseguire delle sessioni di cracking sulla password per recuperare la loro versione in chiaro. Sentitevi liberi di utilizzare qualsiasi dei tool visti nella lezione teorica. L'obiettivo dell'esercizio di oggi è craccare tutte le password.

La prima azione sarà quella di riprendere le password criptate sul sito tramite il comando "UNION".




Copiamo solo le password e le salviamo sul desktop, inserendole in un nuovo documento che chiamiamo 'pp.txt'.

Utilizziamo il comando
‘ **john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5** ./Desktop/pp.txt ‘ e successivamente scriviamo la directory interessata; per decriptare le password dobbiamo inserire il formato md5 che ci servirà per convertirle. Siamo riusciti a trovare 4 su 5 passwords. Per farci mostrare tutto il contenuto (come suggerito nella penultima riga) usiamo “ --show --format=raw-md5 “ e vedremo cosa ci restituirà.




Come si può vedere abbiamo trovato tutte le password.