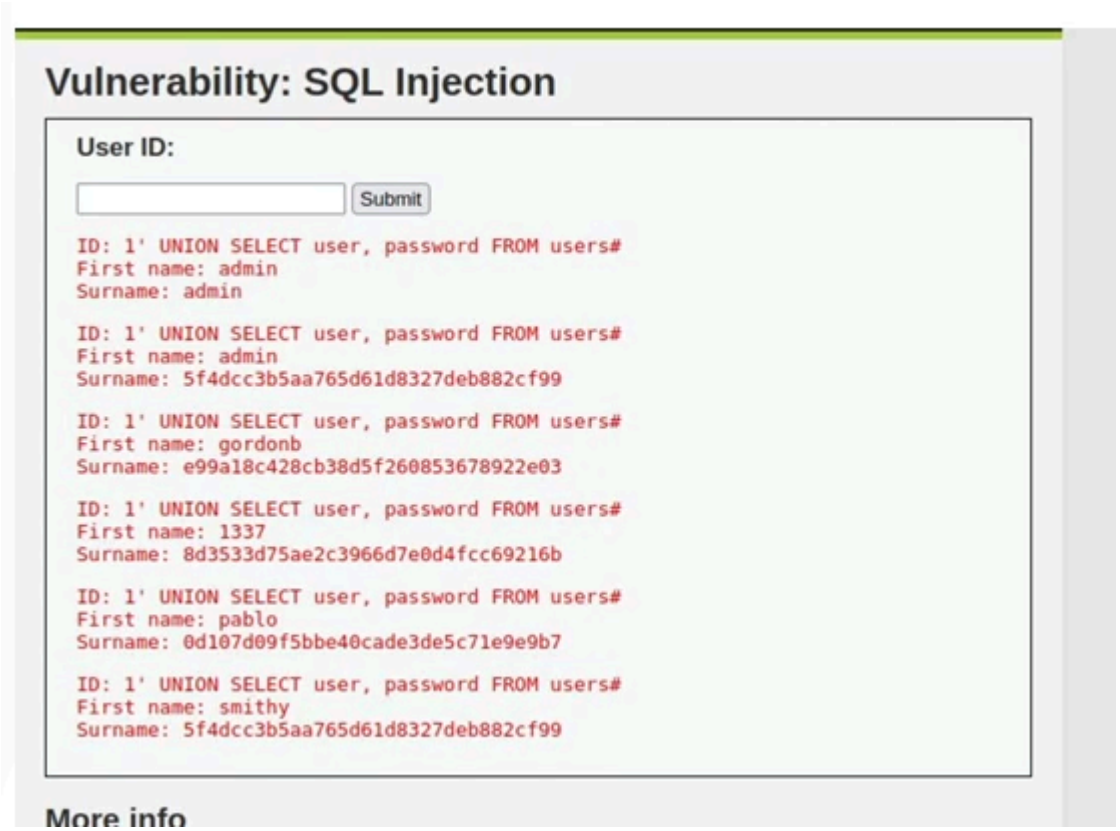
07.11.2024

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.

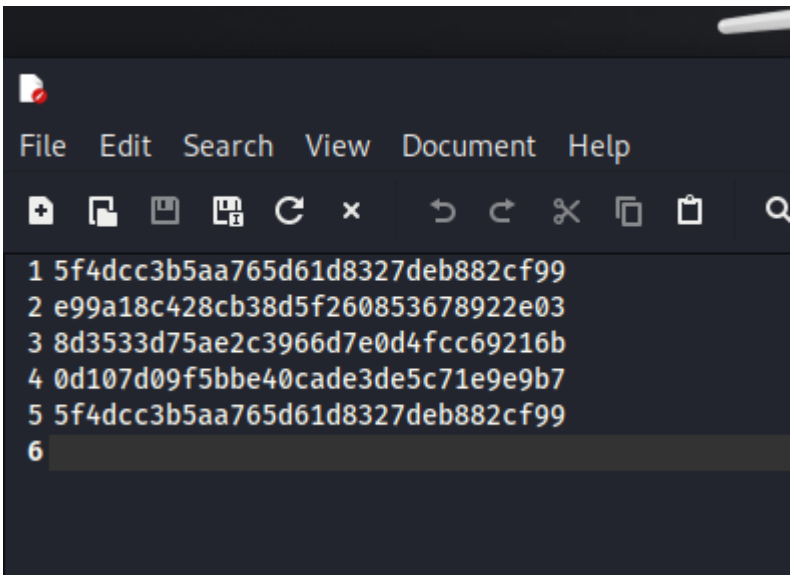
Come da richiesta esercizio dobbiamo andare a crackare delle password in formato Hash MD5.
Innanzitutto dobbiamo procurarci le password e per fare questo chiederemo aiuto al database della nostra DVWA andando alla sezione sql Injection e dando il comando:

1' UNION SELECT user, password FROM users#

Ed otterremo questo:

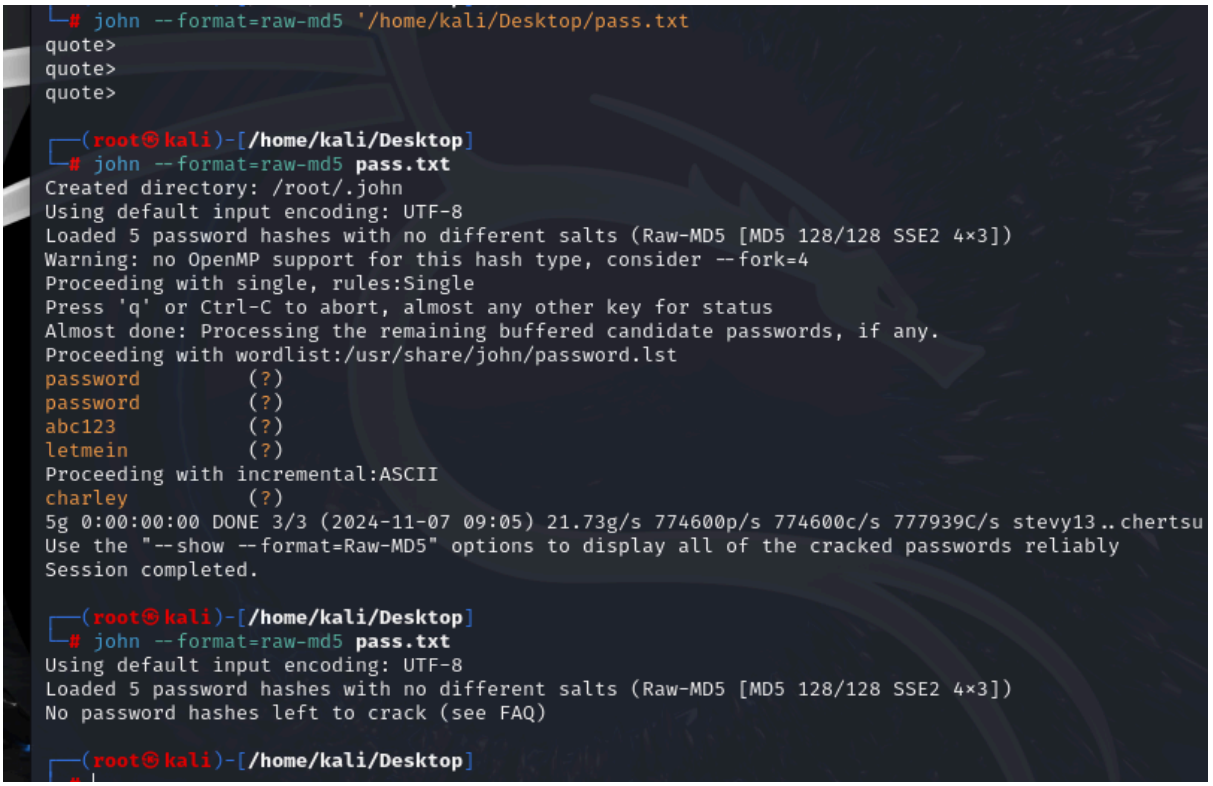


Avendo queste info andremo a creare un file .txt su Kali dove andremo a scrivere tutte le password da crackare:



Apriamo successivamente il terminale nella stessa directory dove abbiamo salvato il file .txt ed eseguiamo il comando

john --format=raw-md5 '/home/kali/Desktop/pass.txt'



ed otterremo così le password in chiaro.