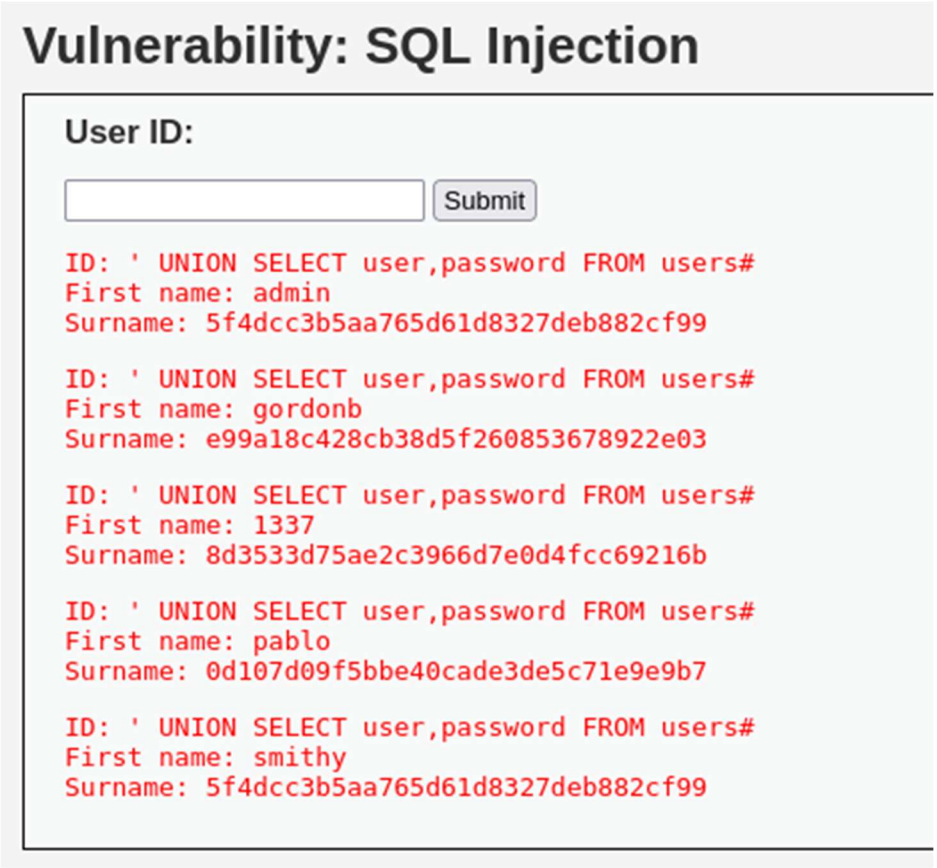
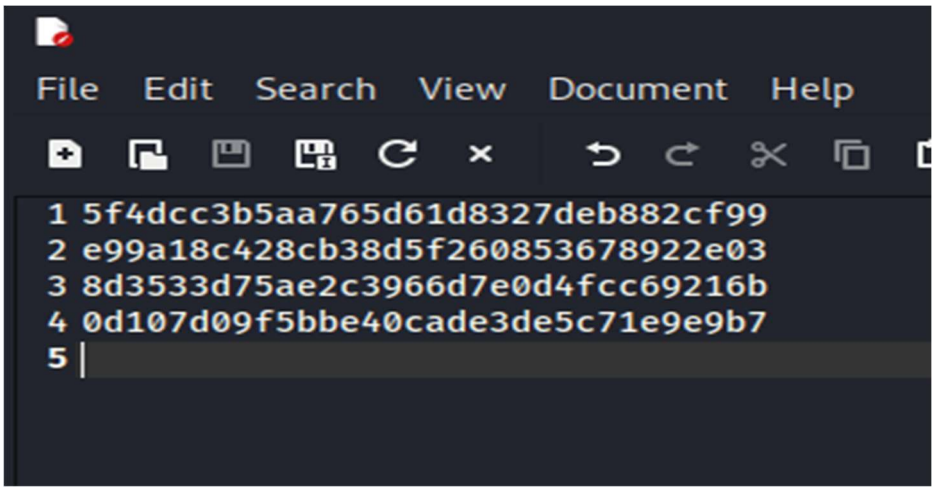
Recuperiamo le password **cifrate** dal database della DVWA tramite **SQL injection**.



Le salviamo nel file **hash.txt**.



Utilizziamo il tool **John the Ripper** da Kali Linux per eseguire un **password cracking** utilizzando il dizionario **rockyou.txt** con le password più comuni (specifichiamo il formato **MD5** di hash poiché sappiamo che le password sono cifrate con quella funzione, altrimenti il tool è comunque in grado di riconoscerlo da solo).

Otteniamo le password **in chiaro**.