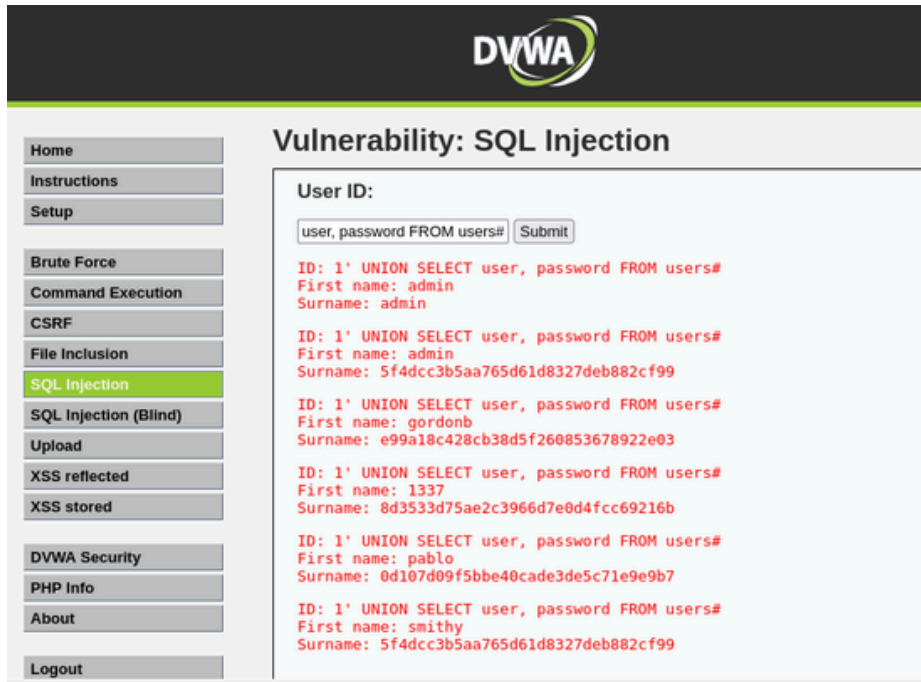


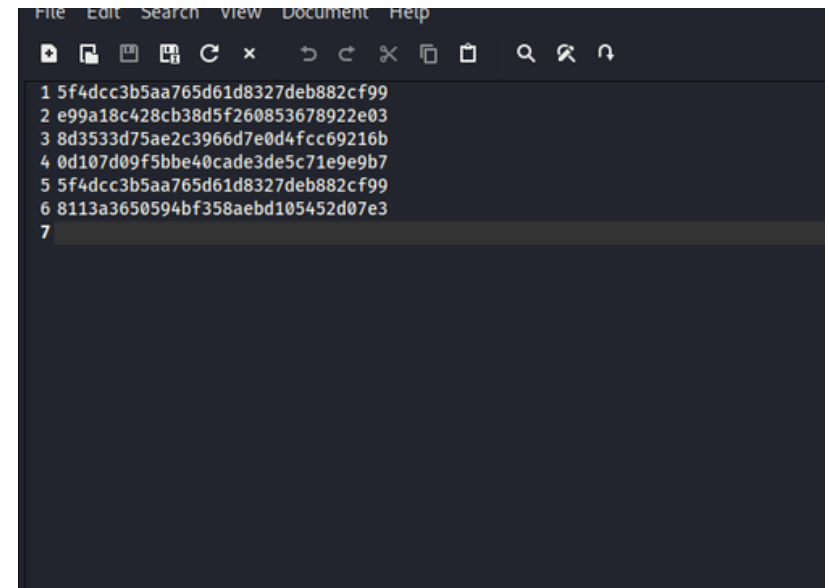
# Pratica S6/L4

## Password Cracking - Recupero delle Password in Chiaro



Utilizziamo la DVWA per simulare un attacco Sql Injection così da recuperare codici Hash

Inseriamo le nostre password all'interno di un file di testo



```
└─$ john --format=raw-md5 '/home/alessio/Desktop/codici_hash.txt'
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
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 14:07) 16.66g/s 594500p/s 594500c/s 599620C/s stevy13..candake
```

Utilizzando il programma **John the Ripper** per decriptare i nostri codici hash, dobbiamo eseguire il seguente comando: **john --format=raw-md5 <percorso\_del\_file\_con\_hash>**

Nel comando, **--format=raw-md5** specifica il tipo di hash (in questo caso MD5) che vogliamo decriptare, mentre **<percorso\_del\_file\_con\_hash>** è il percorso del file che contiene gli hash da decifrare.

Il programma analizzerà gli hash nel file e tenterà di decriptarli utilizzando una libreria interna. A seconda delle risorse disponibili e del dizionario fornito (come **rockyou.txt**), John the Ripper cercherà di indovinare le password corrispondenti e restituirà quelle che riesce a decifrare.