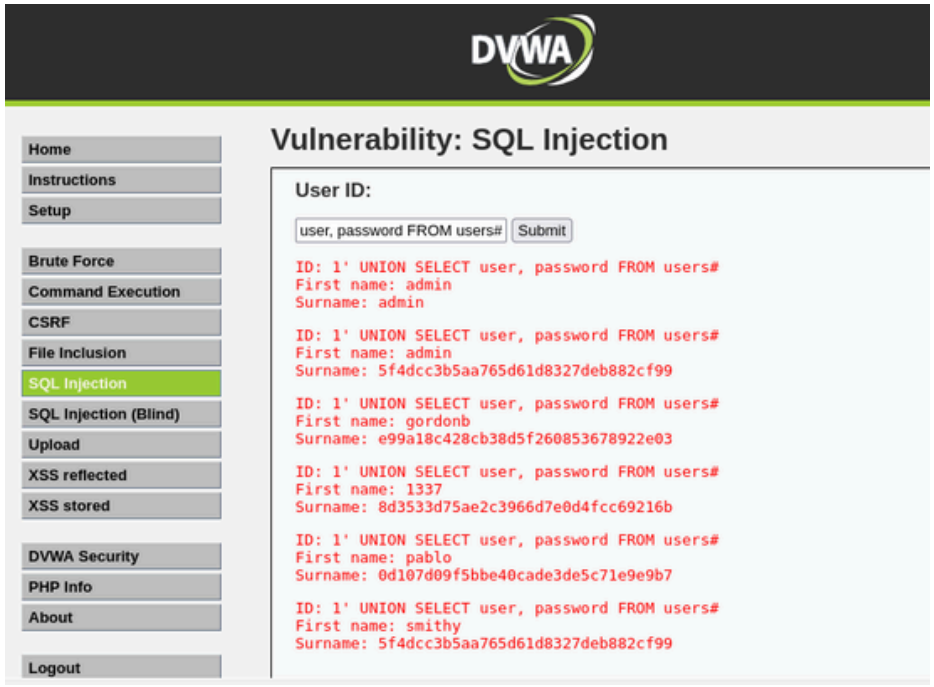
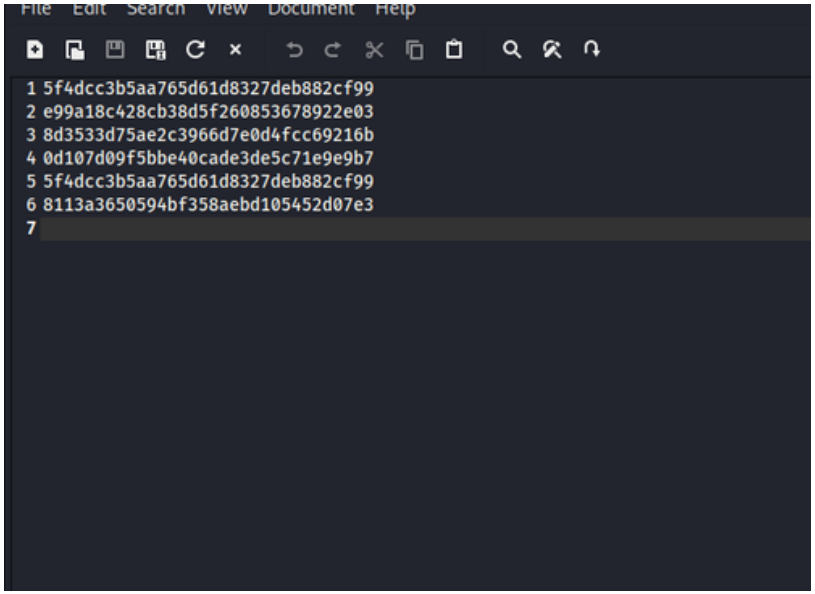
# Pratica S6/L4

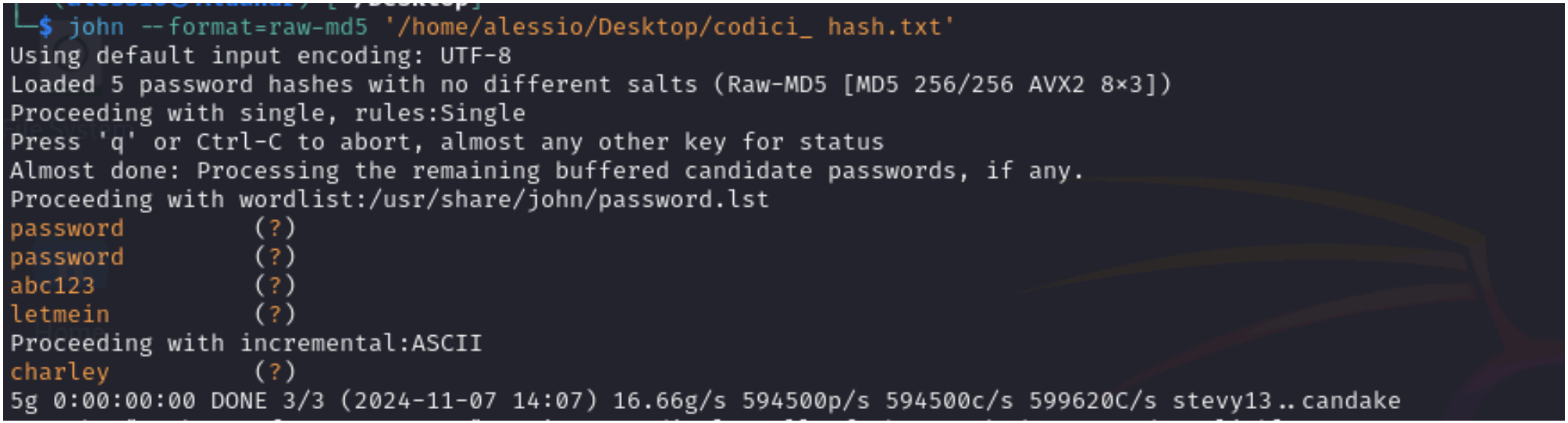
## Password Cracking - Recupero delle Password in Chiaro




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

Inseriamo le nostre password all interno di un file di testo






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.