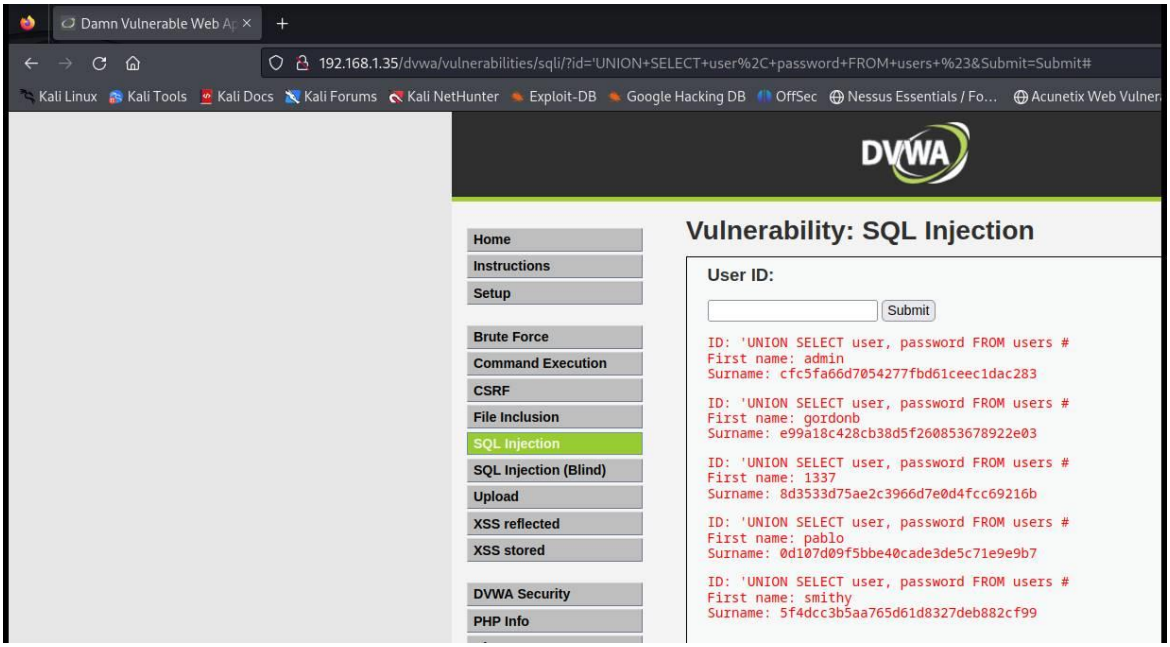
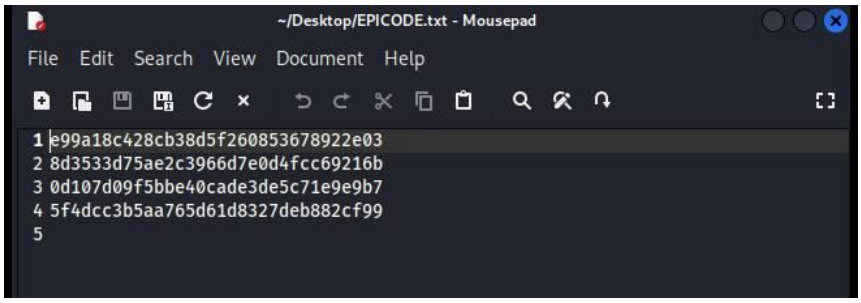
Esercizio 3 Settimana 6

Password Cracking

Oggi andiamo a craccare le password trovate nello scorso esercizio tramite un attacco SQL Injection che sfrutta le vulnerabilità di un server per avere accesso al suo database.
Tramite l'inserimento della stringa *'UNION SELECT user, password FROM users #* in input, riusciamo a risalire a nomi utente e password salvati sulla DVWA:



Qui possiamo notare che le password che dobbiamo svelare sono scritte in codice HASH e, per andarle a decifrare, usiamo JOHN tramite comando *'john –format=RAW-DM5 <FILE.txt>* dove il file scelto non è altro che un testo creato da noi con la lista dei codici hash (va bene anche un file per ogni codice).
A questo punto il programma ha decifrato le nostre password e tramite il comando *'john –show –format=RAW-MD5 <FILE.txt>,* ci mostrerà le password trovate.



.

Le password sono salvate utilizzando degli algoritmi di cifratura a senso unico, ossia non c'è modo di ricostruire la password partendo dalla sua forma crittografica (funzioni di hash).MD5 è una funzione hash molto utilizzata poiché i codici da decifrare sono univoci e una qualsiasi modifica andrà a cambiare il codice. È inoltre progettato per sequenze di 32 caratteri esadecimali.