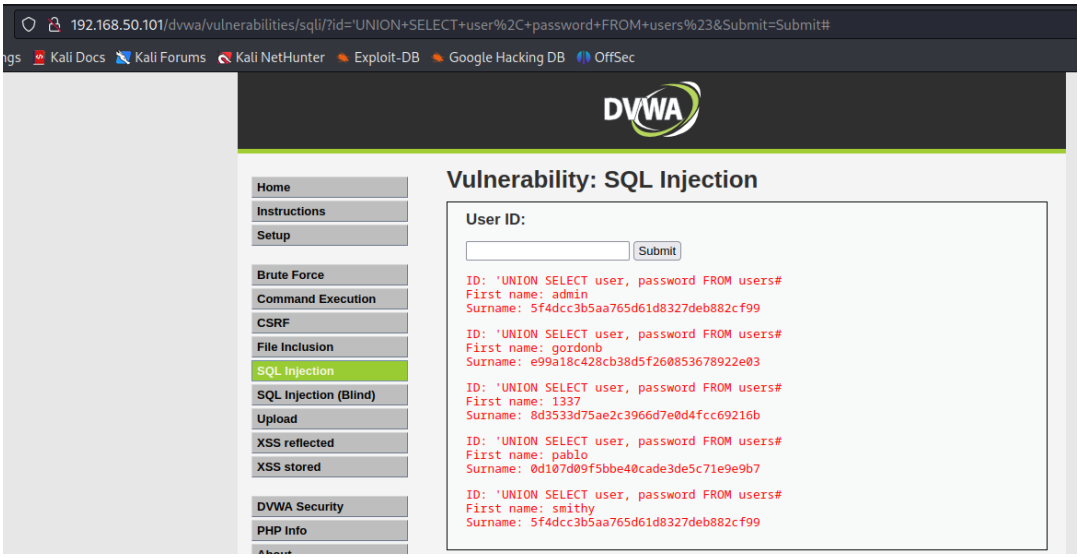
Password cracking

Dopo l'SQL injection fatto ieri, son risalito alle password degli user sulla dvwa.



Successivamente ho preso queste password e le ho inserite in un file txt. Poi con il comando che segue, effettuo un attacco a dizionario.

john –format=raw-md5 –wordlist=/usr/share/wordlists/rockyou.txt hash.txt

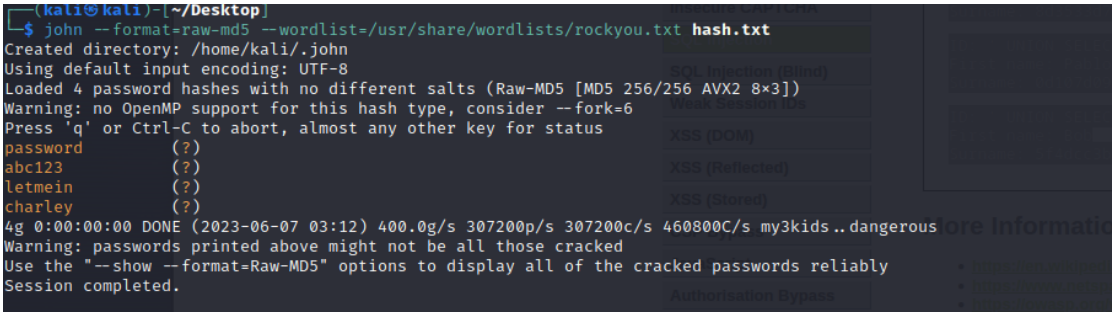
john è un tool di cracking per password, supporta una vasta gamma di algoritmi di hash;

-format=raw-md5 sta ad indicare il tipo di crittografia ;

-wordlist andiamo a prendere la lista a dizionario "rockyou.txt ;

Hash.txt è il file delle password da decriptare.

Come si vede nello screen, il tool ha trovato le password crittografate dal file hash.txt



Una volta effettuata la decriptazione, per visualizzare le password craccate in un determinato file, bisogna eseguire il seguente comando:

john --show –format=raw-md5 hash.txt