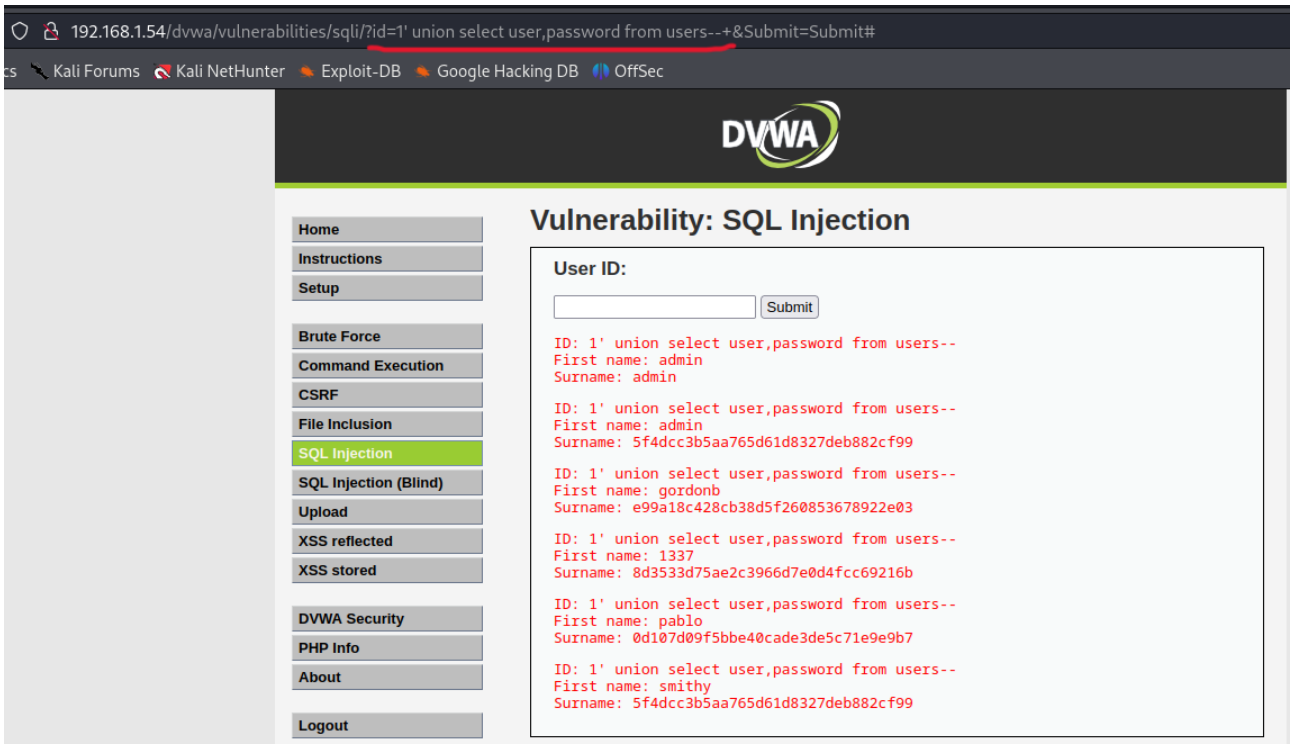
Utilizzando l'attacco SQL Injection (non blind), andiamo a compromettere il database di DVWA:

- Andiamo ad inserire la query nell'URL:

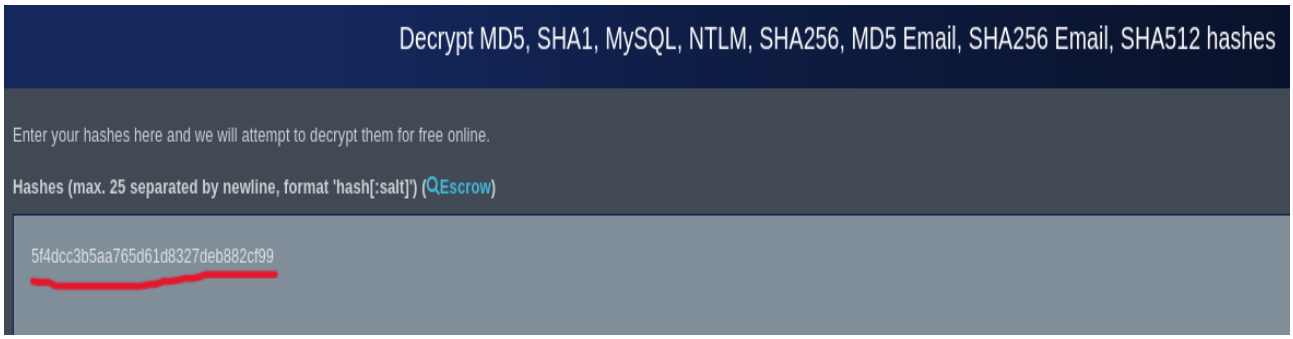
" ?id=1' union select user,password from users--+ "



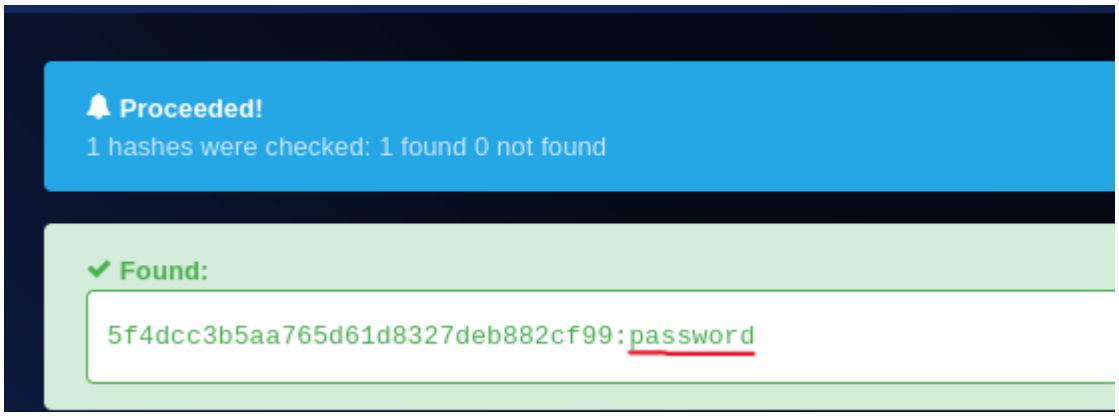
Come vediamo, ci viene restituita la lista di username e password all'interno del database DVWA.

Le password sono riportate in codice hash. Per provare a carpire le password in chiaro, possiamo utilizzare uno dei siti che troviamo online che decriptano il codice hash. Anche se come sappiamo il codice hash non è reversibile, dunque una volta creato non si può più tornare al formato originale, si possono confrontare i codici hash delle password più comuni e vedere se corrispondono a quelle di nostro interesse (ed è proprio quello che fa il sito che siamo andati ad utilizzare).

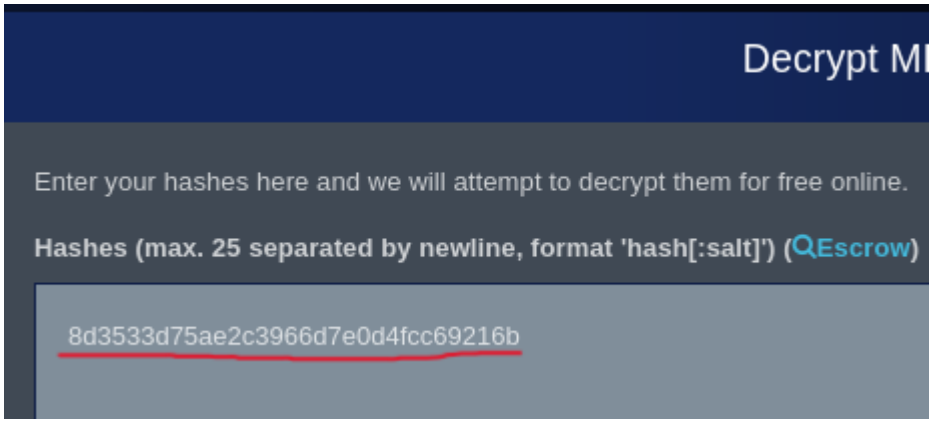
Scriviamo dunque il codice hash della password di 'admin':



Come si può notare, il sito è riuscito a decifrare la password di admin, che è ‘password’:



Proviamo a rifare lo stesso procedimento con il codice hash della password di ‘1337’:



Anche qui, il sito ha decifrato la password di 1337, che è ‘charley’: