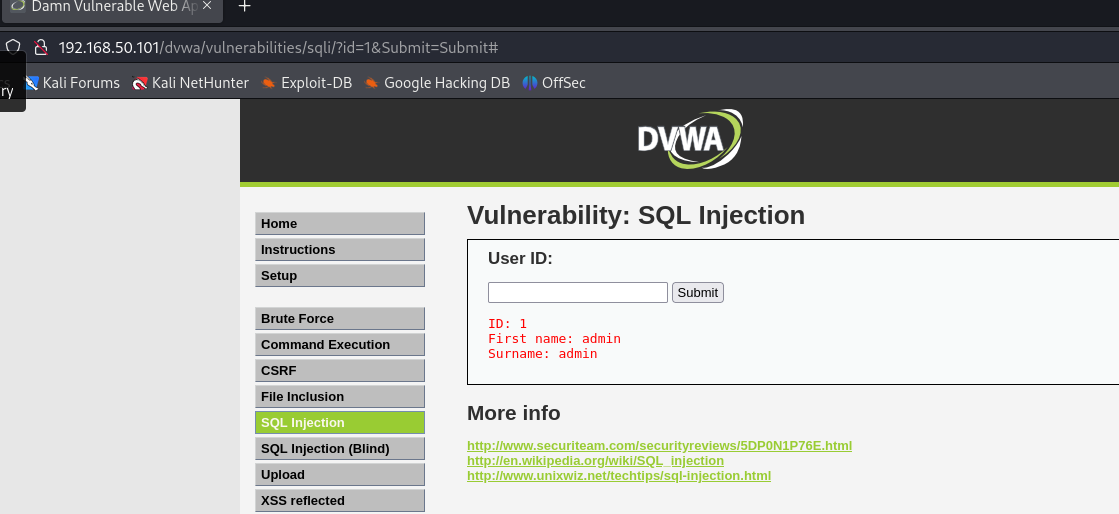
**Esercizio SQL**

Traccia:

Utilizzando l’attacco SQL Injection (non blind), andare a compromettere il database di DVWA.

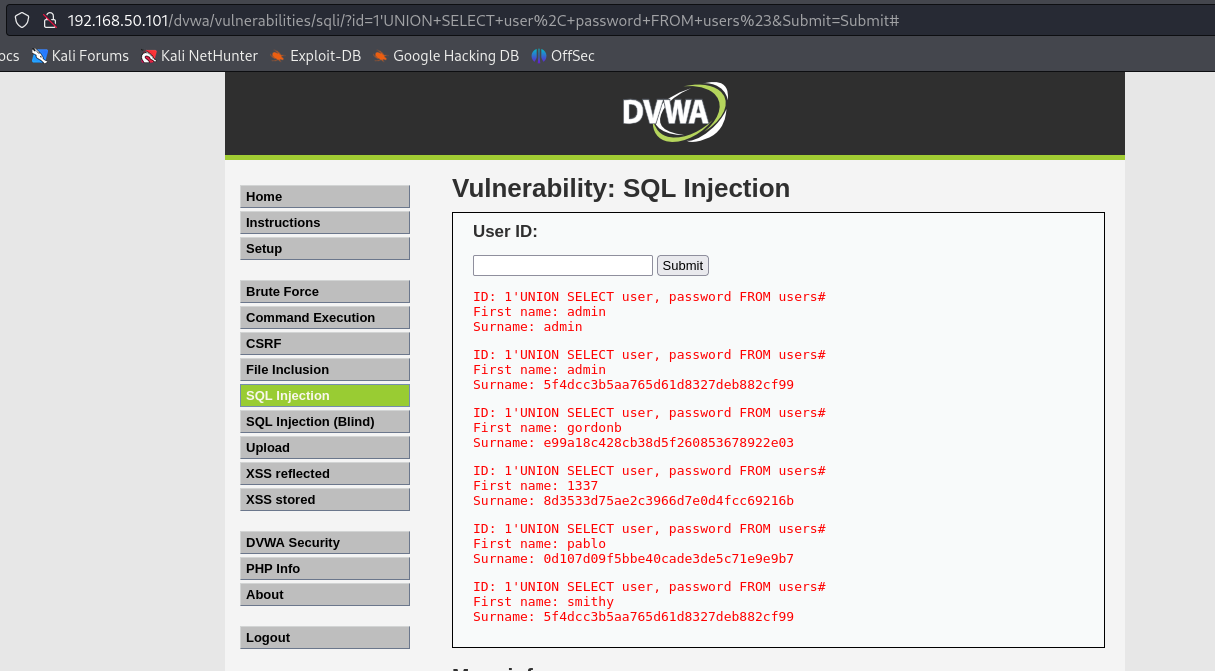
Bonus: Noterete che le password sono in codice hash. Trovare il modo per rendere le password in chiaro.



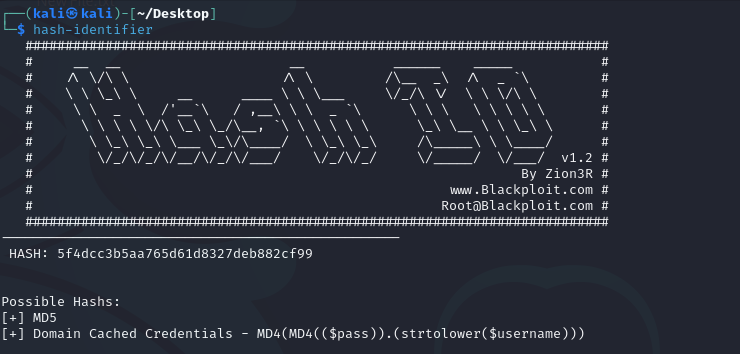
Proviamo ad inserire 1 per capire come funziona l’applicazione. Sembra che l’app ci restituisca un utente da un database in base all’ID.



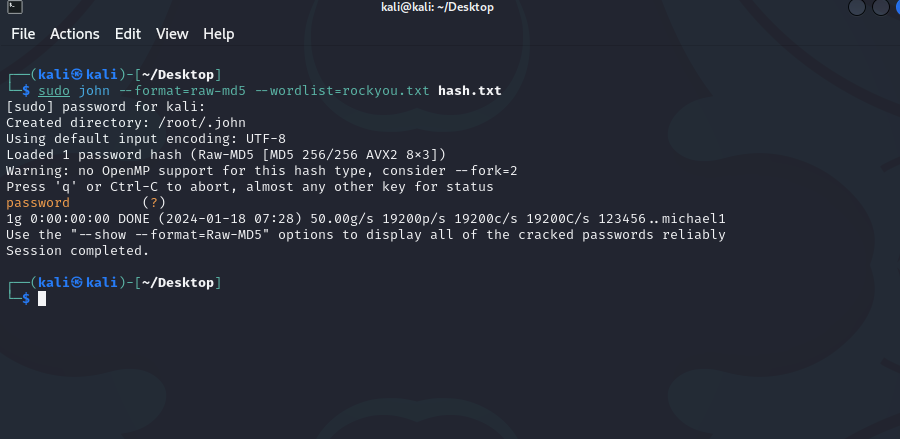
Proviamo ad inserire una condizione sempre vera come ad esempio 1’OR’1’=’1 e vediamo che l’applicazione ci restituisce tutti i risultati per nome e cognome. A questo punto vediamo se siamo in grado di recuperare le password assegnate ad ogni utente.



A questo punto proviamo ad utilizzare una union query: 1'UNION SELECT user, password FROM users# e infatti l’applicazione ci consegna l’ID associato con ogni password, ma ce lo consegna in codice hash.



Usiamo hash identifier per capire che tipo di hash è e scopriamo che è di tipo MD5.



Successivamente con john proviamo a craccare il codice hash per trovare la password di admin e il risultato è: password