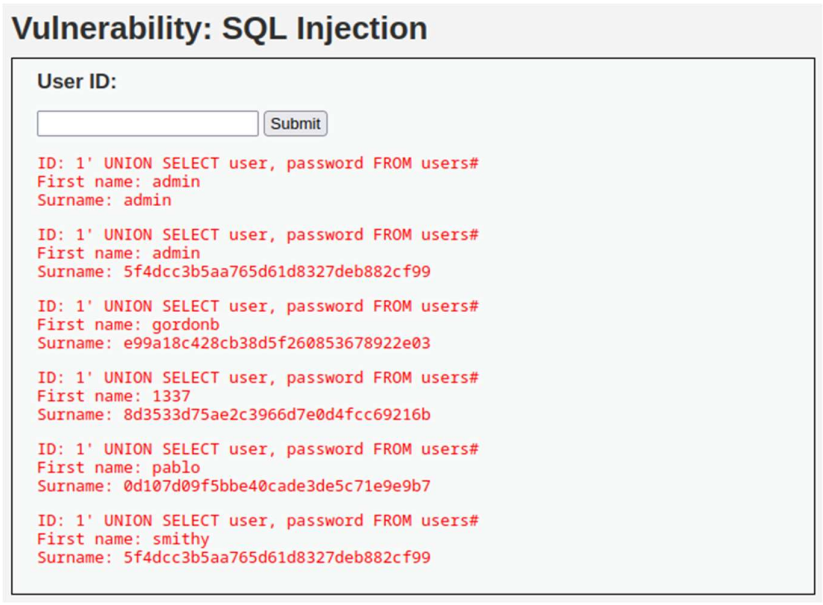
PRATICA S6L3 – Giorgio Trovesi

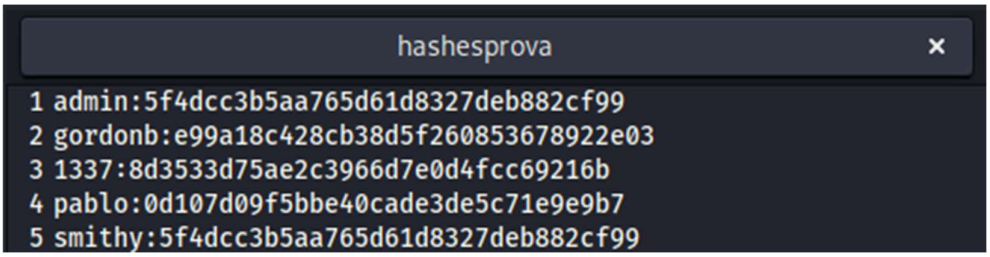
L'obiettivo dell'esercizio di oggi è craccare tutte le password trovate con l'attacco SQL Injection nella DVWA.

Sappiamo che le password trovate sono in hash MD5, cioè un algoritmo che prende in input una stringa e ne produce un'altra a 128bit cioè 32 caratteri esadecimali.

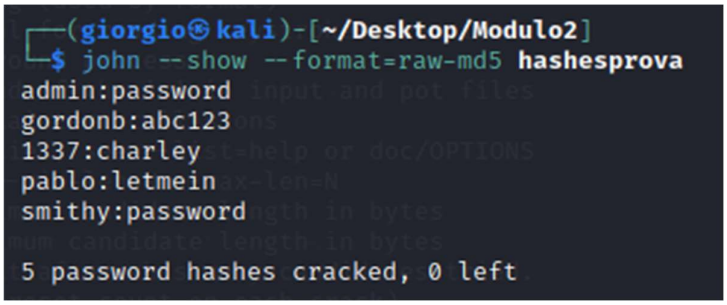
1. Dall'immagine seguente possiamo individuare gli utenti trovati con la relativa password tramite l'attacco SQL Injection.



2. Abbiamo creato un file che incorpori l'accoppiata Username – Password in hash MD5 da poter utilizzare successivamente con il tool John The Ripper.



3. Tramite l'utilizzo di John, abbinato alle options "show" e "format" siamo riusciti a decriptare le password di ciascun utente come si può constatare nell'immagine seguente.



4. Essendo in possesso delle informazioni di login, abbiamo testato che effettivamente fossero valide, eccone un esempio a prova di ciò.