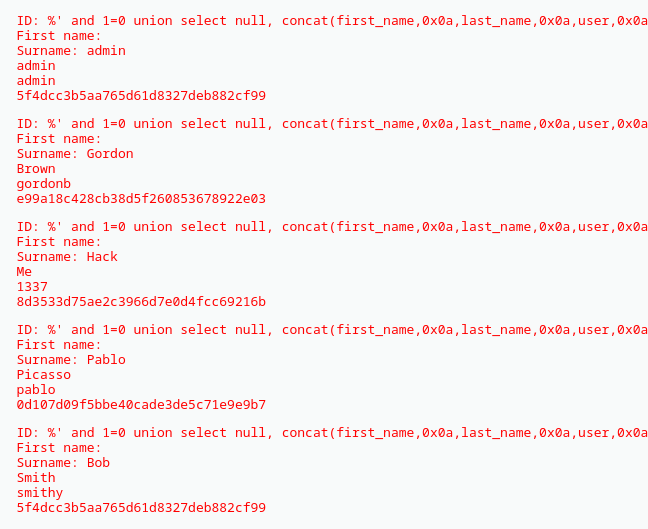
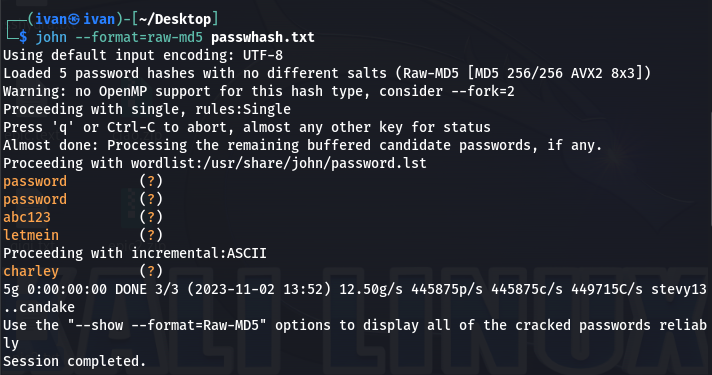
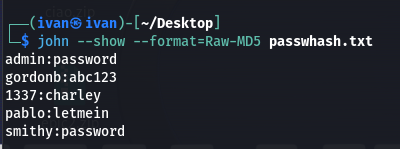
**PASSWORD CRACKING**

Nell’esercizio precedente abbiamo visto come sfruttare un attacco SQL injection per recuperare le password degli utenti di un determinato sistema.  
Facendo particolare attenzione, non hanno l’aspetto di password in chiaro, ma sembrano più hash di password MD5. Siamo andati quindi ad eseguire un cracking delle password per poterle vedere in chiaro.



**1) John The Ripper**

Abbiamo utilizzato questo tool in modo da vedere in chiaro le password che precedentemente erano in hash. Possiamo notare come le password vengano crittografate casualmente.

Utilizziamo quindi il comando “john –showformat=Raw-MD5” per farcele stampare nell’ordine che noi avevamo impostato precedentemente.

Provando ad inserire queste coppie di credenziali in DVWA, possiamo notare come accediamo alla homepage di ogni user stampato.