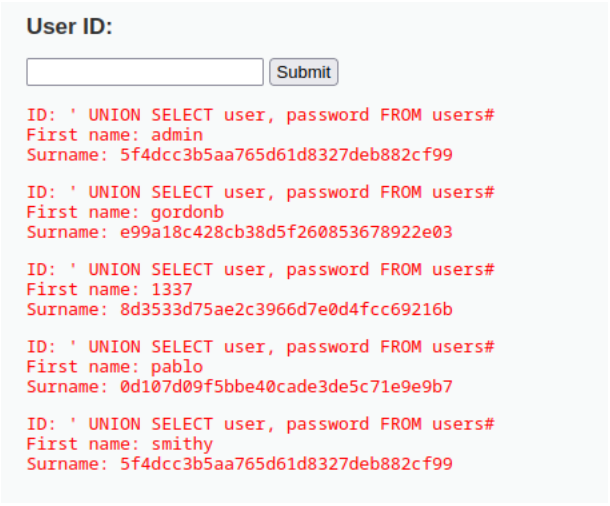

Dopo aver trovato le password tramite sql injection ci rendiamo conto che le password sono cifrate e dobbiamo quindi decriptarle; per farlo ho usato crackstation, il quale ci restituisce le password leggibili e ci dice che il metodo di cifratura era l'md5 ovvero una funzione di hash crittografico ampiamente utilizzata per convertire dati arbitrari in una rappresentazione di lunghezza fissa, nota come hash. L'hash MD5 risultante è un valore univoco per un dato input, il che significa che anche una piccola modifica nei dati di input produrrà un hash completamente diverso. Una volta creato l'hash neanche il sistema operativo ha bisogno di sapere la password in chiaro infatti quando l'utente esegue l'accesso il SO converte la password in chiaro in un hash e lo confronta con l'hash registrato.

Vediamo quindi i risultati degli hash: Il primo risultato è la password dell'user ID *admin*

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

Il risultato è la password dell'user *pablo*

Hash	Type	Result
0d107d09f5bbe40cade3de5c71e9e9b7	md5	letmein

Abbiamo poi il risultato dell'user *1337*

Hash	Type	Result
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley

Il risultato dell'user *gordonb*

Hash	Type	Result
e99a18c428cb38d5f260853678922e03	md5	abc123

Ed infine il risultato dell'user *smithy*

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

Grazie a queste password è possibile eseguire il login dei vari user.