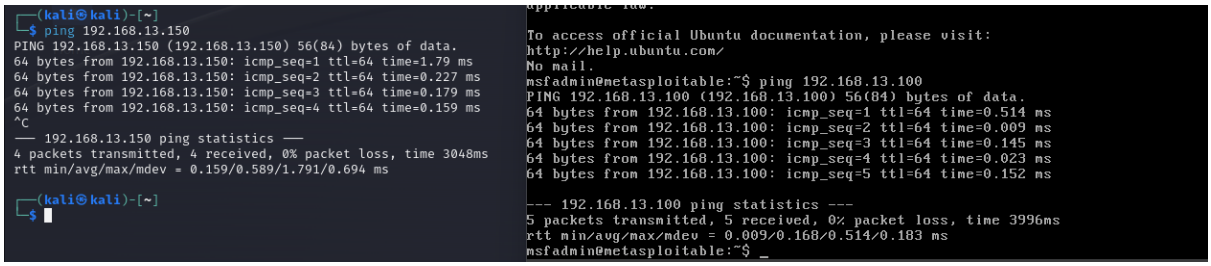
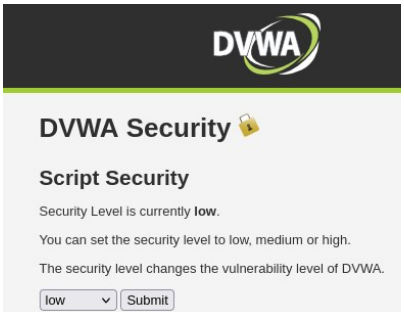
SQLi

L obbiettivo è di trovare le credenziali di accesso dell utente Pablo Picasso della DVWA

Per farlo ho prima configurato le macchine in modo tale che comunicassero

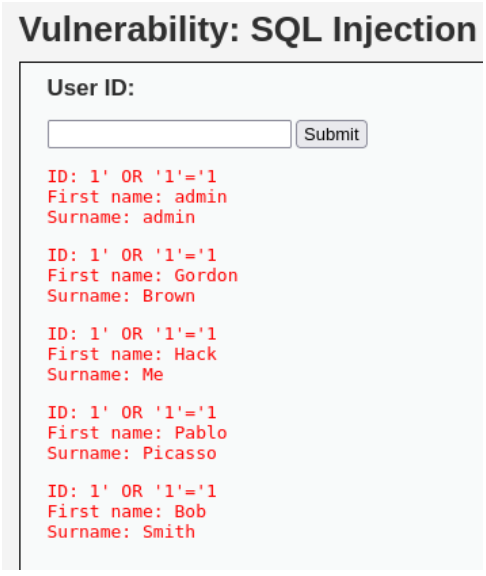


Dopo di che ho impostato la sicurezza della dvwa su low per poter eseguire la SQLi



Per trovare i nomi degli utenti ho iniettato una query con condizione “ sempre vera “con il codice

1' OR '1'='1



Dopo avere trovato il mio utente target “ Pablo Picasso “

dovevo trovare la Pw di accesso , per farlo ho usato un altra Query :

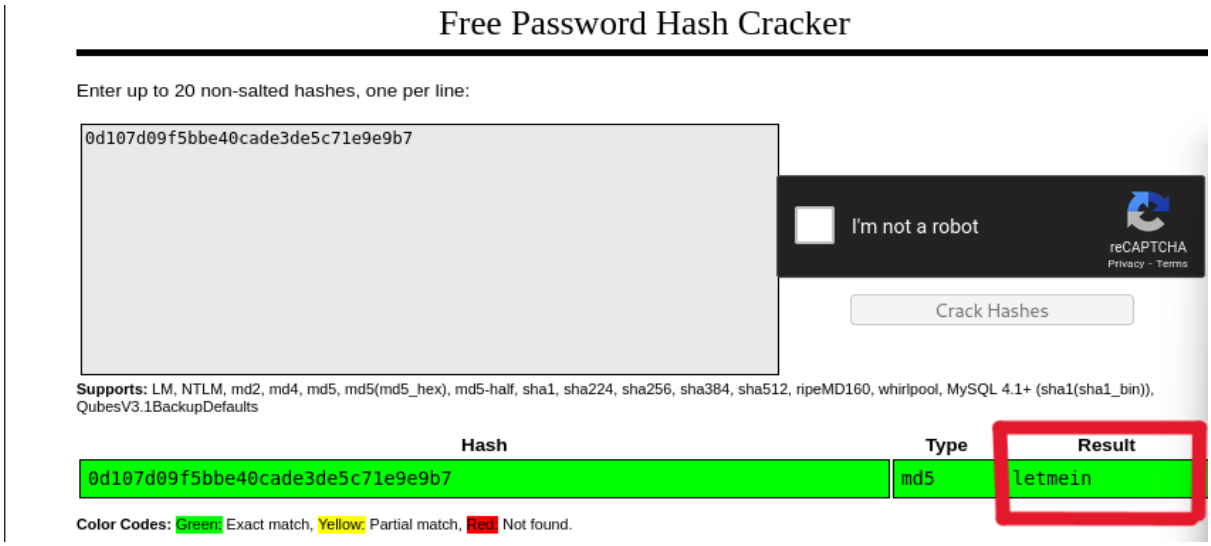
' UNION SELECT user, password FROM users#

```
ID: ' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
```

ottenendo il risultato nella foto soprastante

Il problema adesso era trovare la Password in chiaro , per risolvere questo problema ho utilizzato il sito web : https://crackstation.net/ - copiando l hash trovato precdentemente e incollandolo

CrackStation utilizza delle tabelle di ricerca precalcolate per decifrare gli hash delle password , quindi una volta incollato ha effettuato una ricerca che essendo andata a buon fine mi ha restituito la password



Per accertarmi che fosse corretta ho provato a ri effettuare l ' accesso alla DVWA utlizzando

User : Pablo Password : letmein - esito nelle foto sottostanti