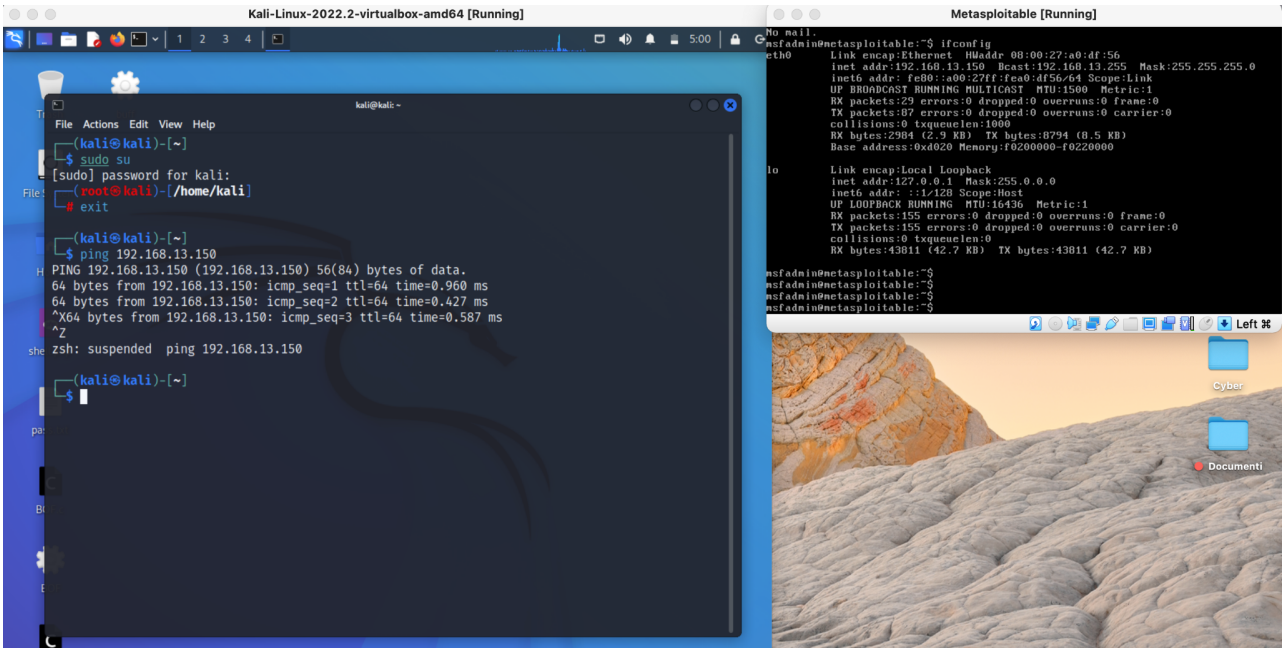
SQL Injection



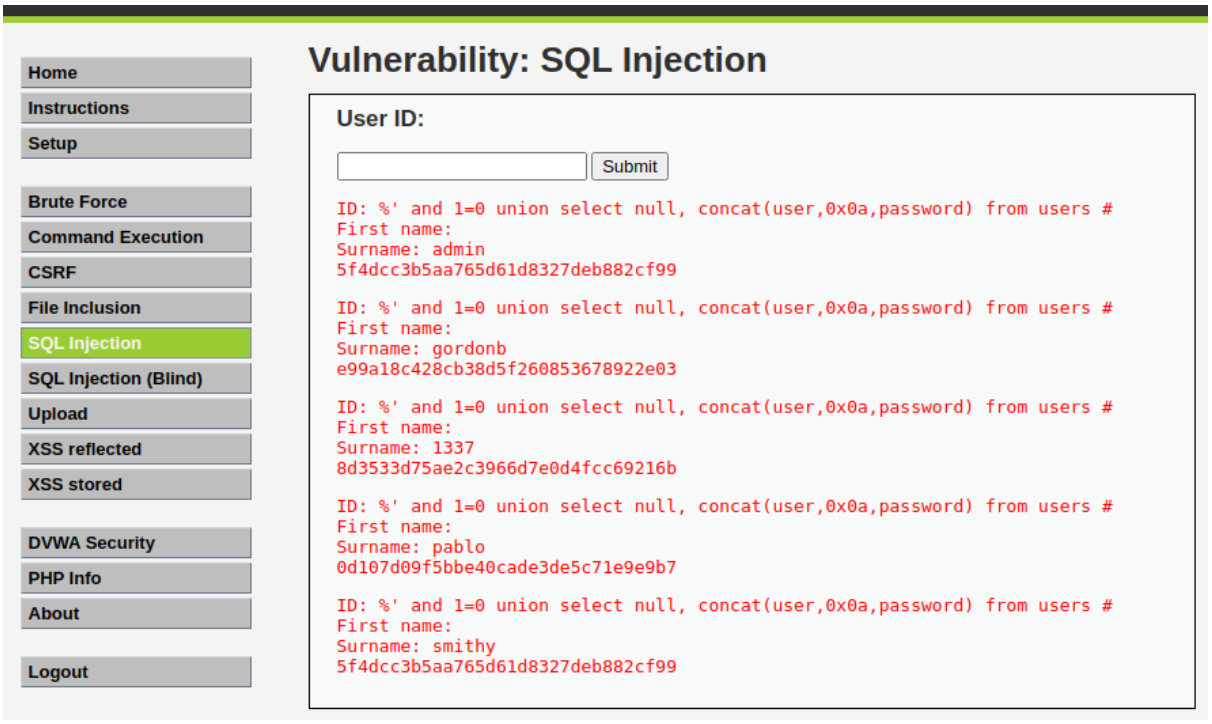
L'obiettivo di oggi è quello di recuperare la password in chiaro dell'utente Pablo Picasso tramite la tecnica del SQL injection.

SQL injection: solitamente un'applicazione Web utilizza uno o più database di backend per salvare i dati che elabora. Per interagire con i database,le applicazioni web utilizzano lo <structured query language> o SQL.
La SQL injection è una tecnica di code injection, usta per attaccare applicazioni che gestiscono dati attraverso database relazionali sfruttando il linguaggio SQL.

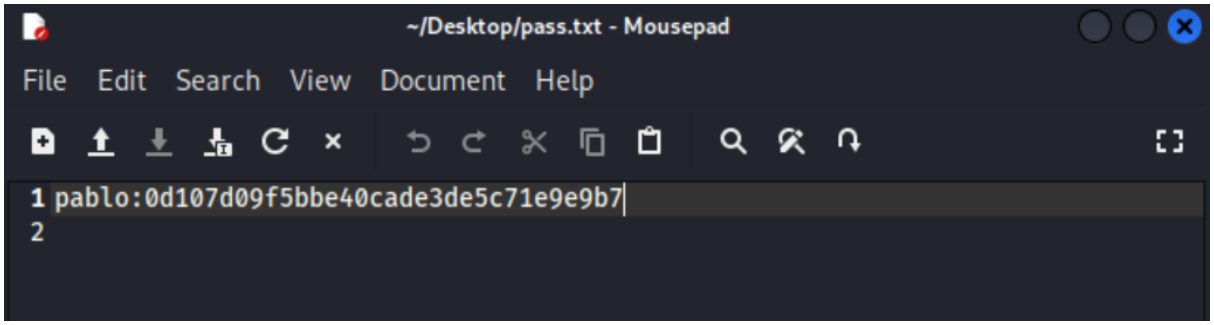
Come primo passo cambiamo gli indirizzi IP delle due macchine:

- Kali -> 192.168.13.100
- Metasploitable -> 192.168.13.150

Dopo aver impostato su 'low' la sicurezza della DVWA, ci siamo spostati sulla tab SQL injection e tramite il codice *''%' and 1=0 union select null, concat(user,0x0a,password) from users#''* abbiamo rilevato i codici hash delle password di ciascun utente.



Una volta ricavato il codice hash dell'utente Pablo, andiamo a realizzare un file .txt in cui andiamo ad associare l'utente con il suo codice hash in modo che '*John the Ripper*' possa decriptare in seguito il formato md5.



Andiamo ad avviare il tool JtR specificandone il formato ed il file da dove decriptare il codice. Siamo così riusciti a ricavare la password in chiaro di Pablo, ovvero *'letmein'*.