Progetto Modulo 4.

Esercizio 1

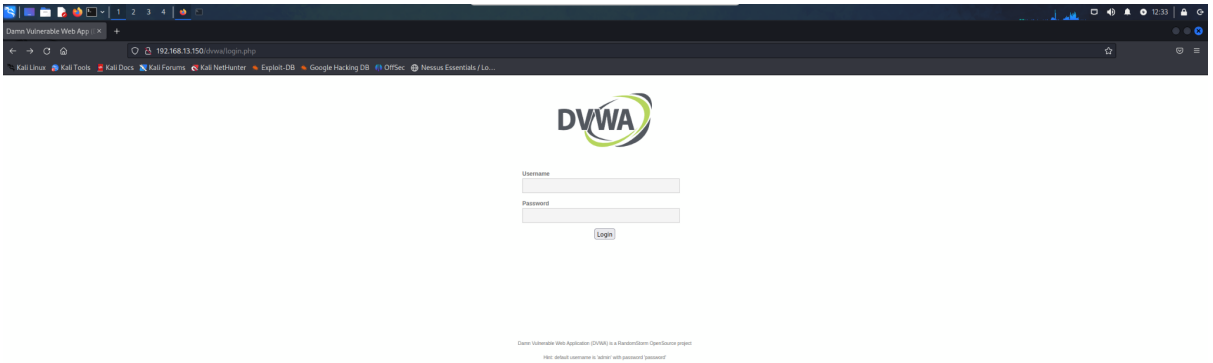
Traccia : Utilizzando le tecniche viste nelle lezioni teoriche, sfruttare la vulnerabilità SQL injection presente sulla web application DVWA per recuperare in chiaro la password dell'utente Pablo Picasso.

Requisiti Laboratorio

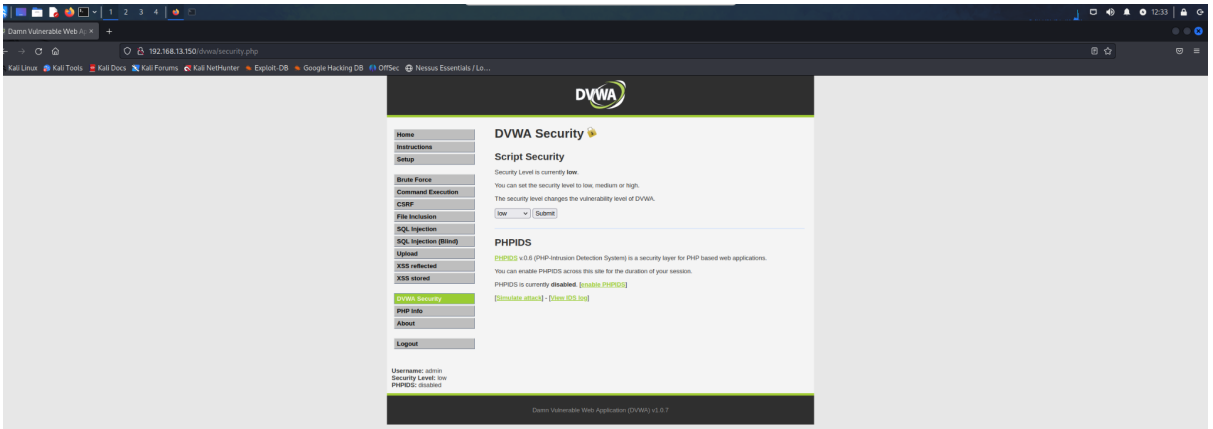
Livello difficolta DVWA : LOW
IP Kali : 192.168.13.100/24
IP Metasploitable _ 192.168.13.150/24

Com richiesto nella traccia in questo esercizio andremo a sfruttare la vulnerabilità SQL Injection presente sulla Web Application DVWA.
Partiamo dalla configurazione del laboratorio :

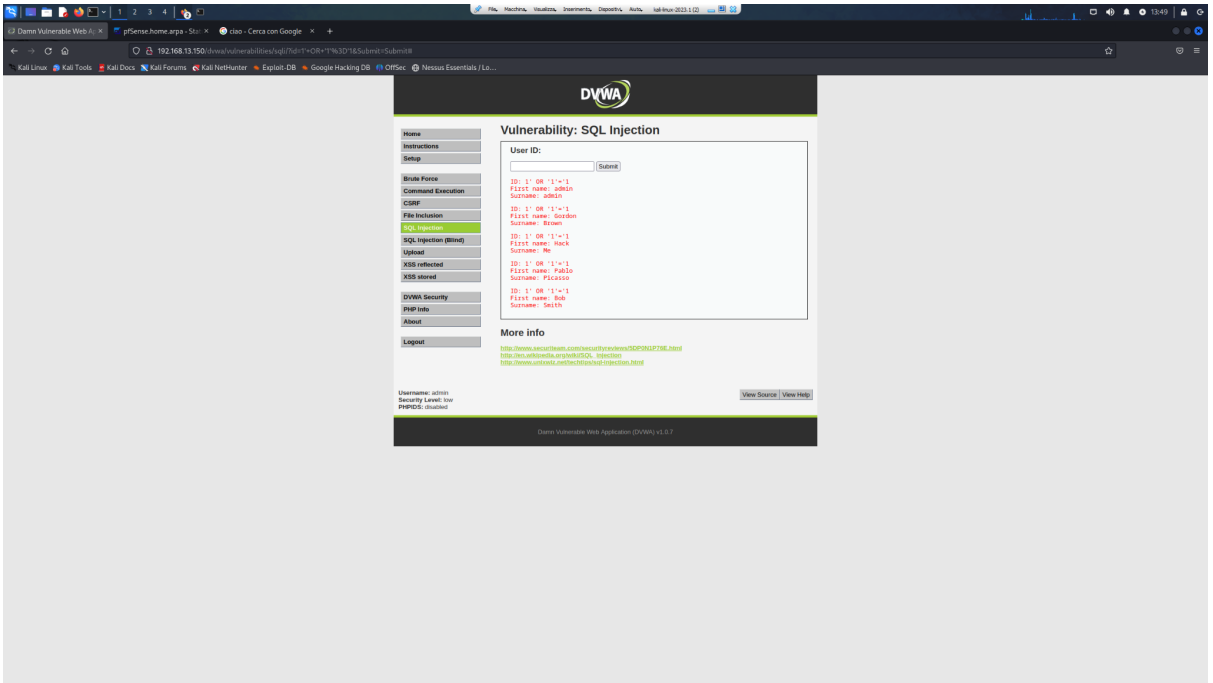
Dopo aver impostato l'ip su Metasploitable e Kali, impostiamo il security level della DVWA a LOW.
Possiamo farlo dopo aver digitato sul browser l'indirizzo ip della nostra macchina metasploitable.



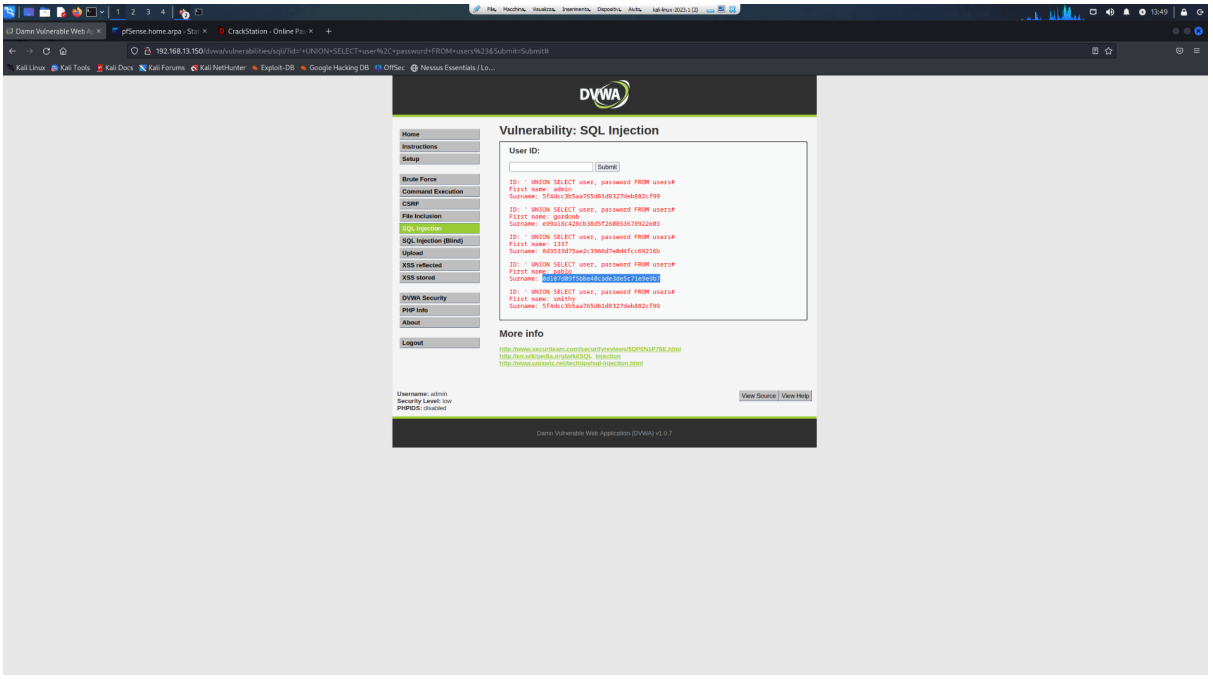
Cerchiamo DVWA Security nel menù a sinistra e dopo aver cliccato impostiamo a low e clicchiamo submit.



Dovendo sfruttare l' SQL injection , cerchiamo nel menu a sinistra la voce corrispondente e clicchiamo.
Sfruttando una query sempre vera tentiamo di recuperare First Name e Surname delle entry del database per poter poi cercare la password dell'utente Pablo Picasso.
La query utilizzata è -> **1' OR '1'='1**



Adesso che sappiamo che l'utente Picasso è l'unico a chiamarsi Pablo in questo database,sfruttiamo una UNION QUERY dove andremo a selezionare il first name e ci faremo restituire dal database anche la password.
Query utilizzata -> **' UNION SELECT user, password FROM users#**



Come possiamo vedere siamo riusciti ad imbrogliare il database con questa query e ci siamo fatti restituire al posto del parametro surname la password che però non è in chiaro.
A questo punto possiamo usare un utility come **John The Ripper** su kali, oppure andare su un sito web come **crackstation** che decifrerà l'hash usato per nascondere la password e ci verrà restituita la password in chiaro dell'utente Pablo Picasso