DVWA Metasploitable

Requisiti laboratorio :

Livello difficoltà DVWA : LOW

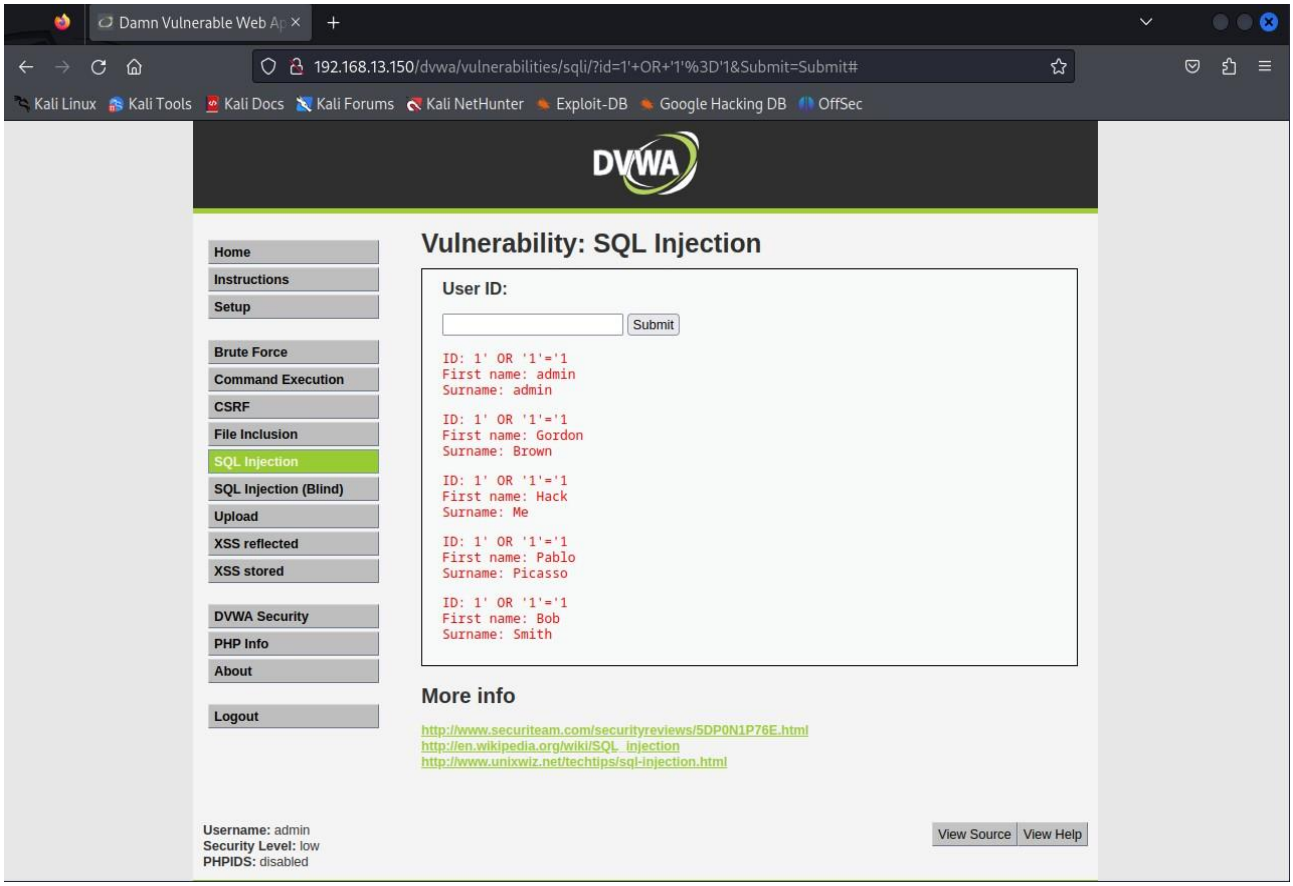
IP Kali : 192.168.13.100/24

IP Metasploitable : 192.168.13.150/24

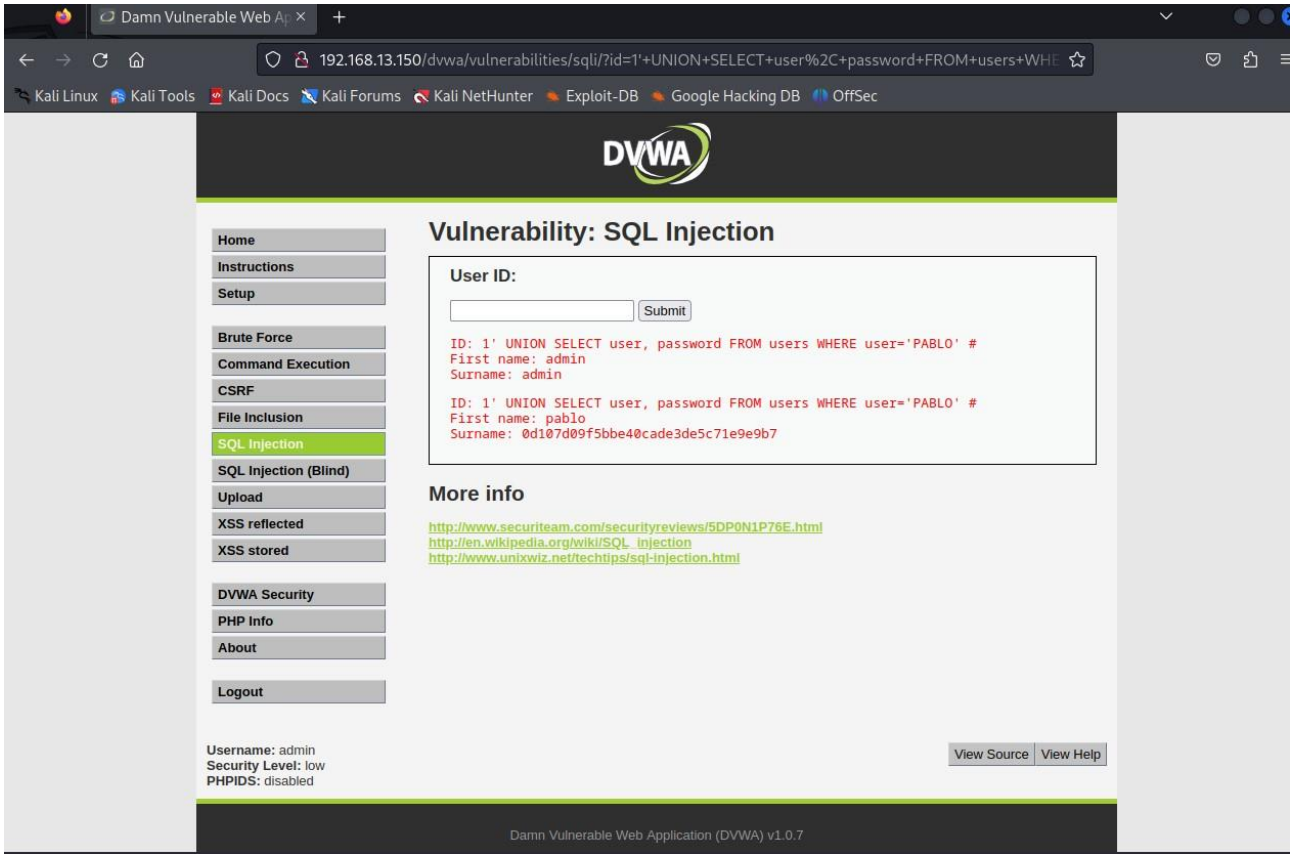
Richiesta:

Recuperare in chiaro la password PABLO PICASSO La stringa 1’ OR ‘1’ =’1 cerca di manipolare una query SQL all’interno dell’applicazione vulnerabile (DVWA) in modo che la condizione 1’ OR ‘1’ =’1 sia sempre vera, il che, consente di ottenere accesso non autorizzato sul database sottostante.

Con questa stringa otteniamo il controllo degli utenti.



La stringa 1’ UNION SELECT user, password FROM users WHERE user=’PABLO’ # cerca di sfruttare una possibile vulnerabilità all’interno dell’applicazione DVWA per estrarre informazioni sul nome utente con il nome ‘PABLO’ dalla tabella ‘users’ nel database.



Il comando sudo john – format=raw-md5 – wordlist=/usr/share/wordlists/rockyou.txt prove.txt è un comando che utilizza l'utility cracking delle password Jhon the Ripper per tentare di decifrare le password contenute nel file 'prove.txt' utilizzando un attacco basato su dizionario.

Nel file prove.txt è contenuta la password trovata con il comando ' 1' UNION SELECT user, password FROM users WHERE user='PABLO' # 'nella sezione 'SURNAME'

Il comando eseguirà un attacco basato su dizionario, utilizzando il dizionario “rockyou.txt” contro le password hash nel file “prove.txt”. Se riesce a trovare una corrispondenza tra una password hash e una parola chiave nel dizionario, la password originale sarà decifrata e visualizzata a schermo.