Report sul Laboratorio di Vulnerabilità - DVWA Exploitation

Data 09/01/23

Guglielmo Carratello

Obiettivo

Contestualizzazione della configurazione del laboratorio virtuale.

Scopo del laboratorio: Raggiungere la DVWA da Kali Linux, assicurando la comunicazione e configurando il livello di sicurezza a "LOW".

Sfruttare le vulnerabilità XSS reflected e SQL injection come visto a lezione.

Configurazione del Laboratorio Virtuale:

Iniziamo configurando Kali Linux (attaccante) e la macchina Metasploitable2 con la rispettiva DVWA (macchina bersaglio), in modo che le due macchine siano sulla stessa rete e di conseguenza consentire la comunicazione tra le due macchine.

Esecuzione del comando ping per verificare la connettività tra Kali Linux e DVWA.

Gli indirizzi IP sono:

- 192.168.32.100 (Kali Linux)
- 192.168.32.102 (Meta)

Raggiungere la DVWA:

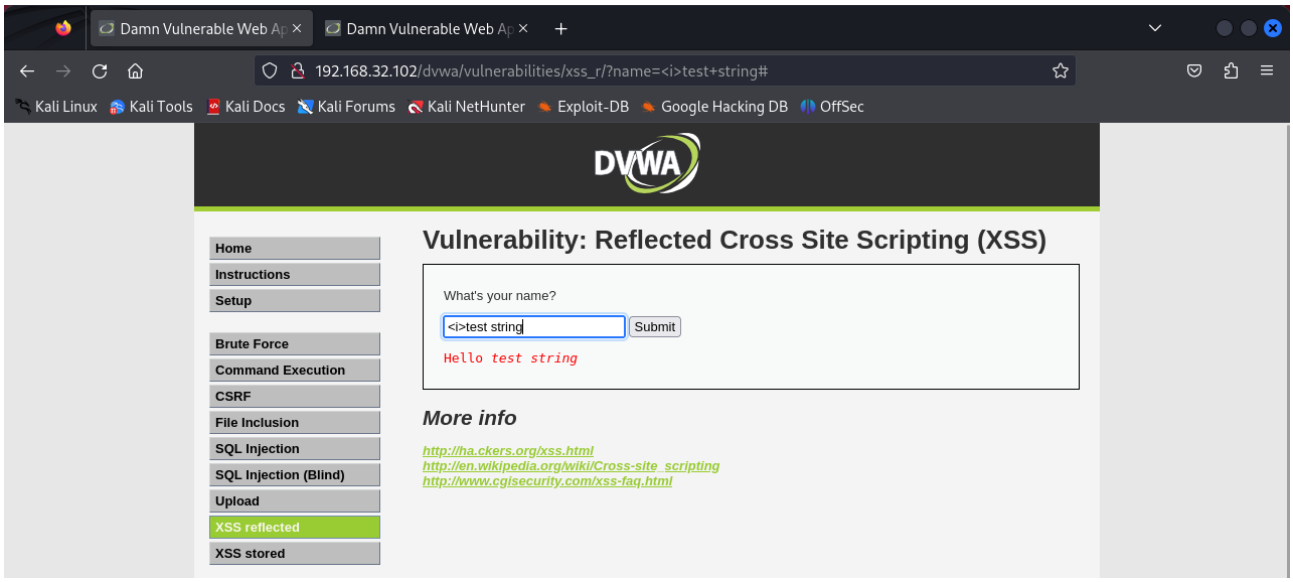
Utilizziamo il browser da Kali Linux per accedere all'interfaccia web della DVWA inserendo l’indirizzo IP di meta nella barra di ricerca del browser.

Accediamo alla DVWA ed impostiamo il livello di sicurezza a "LOW" all'interno della DVWA.

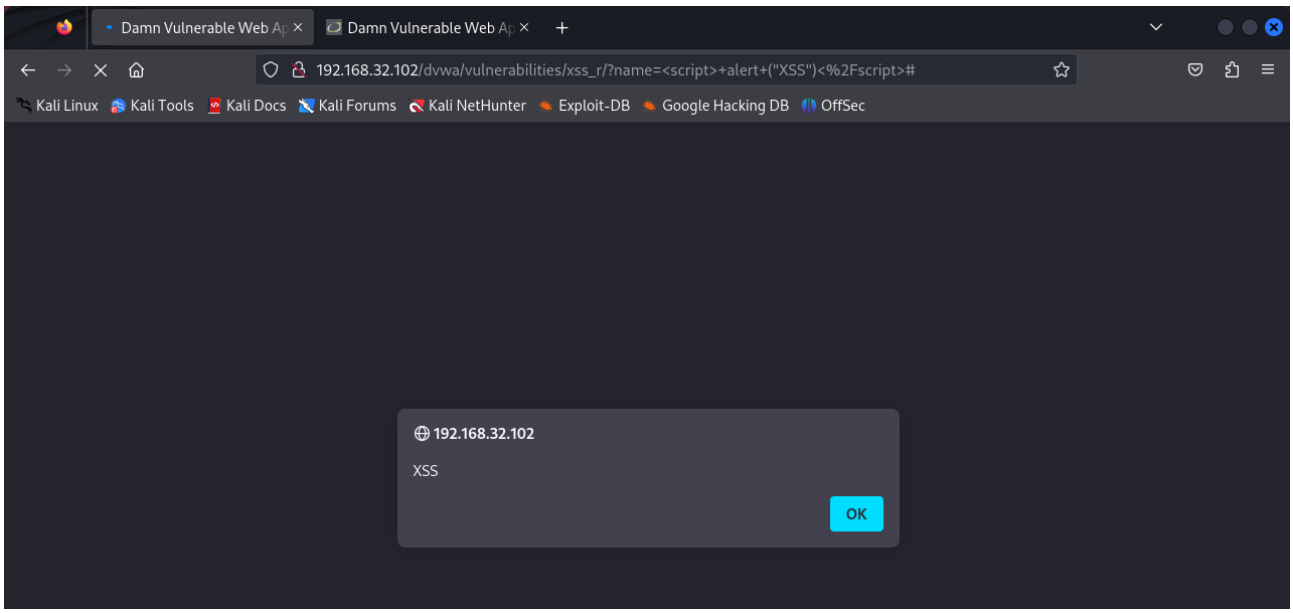
Sfruttamento della Vulnerabilità XSS

Clicchiamo sulla sezione all'interno della DVWA per l'iniezione di script XSS reflected. Utilizziamo lo script visto a lezione <i> test string questo una volta interpretato dalla pagina web mostra in corsivo il testo che in questo caso è “test string”.

Dimostrazione della capacità di eseguire uno script arbitrario attraverso la vulnerabilità XSS.



Un altro script utilizzato per l’attacco XSS ha permesso di creare una finestra di pop-up con all’interno un messaggio, <script> alert(“XSS”) </script>.

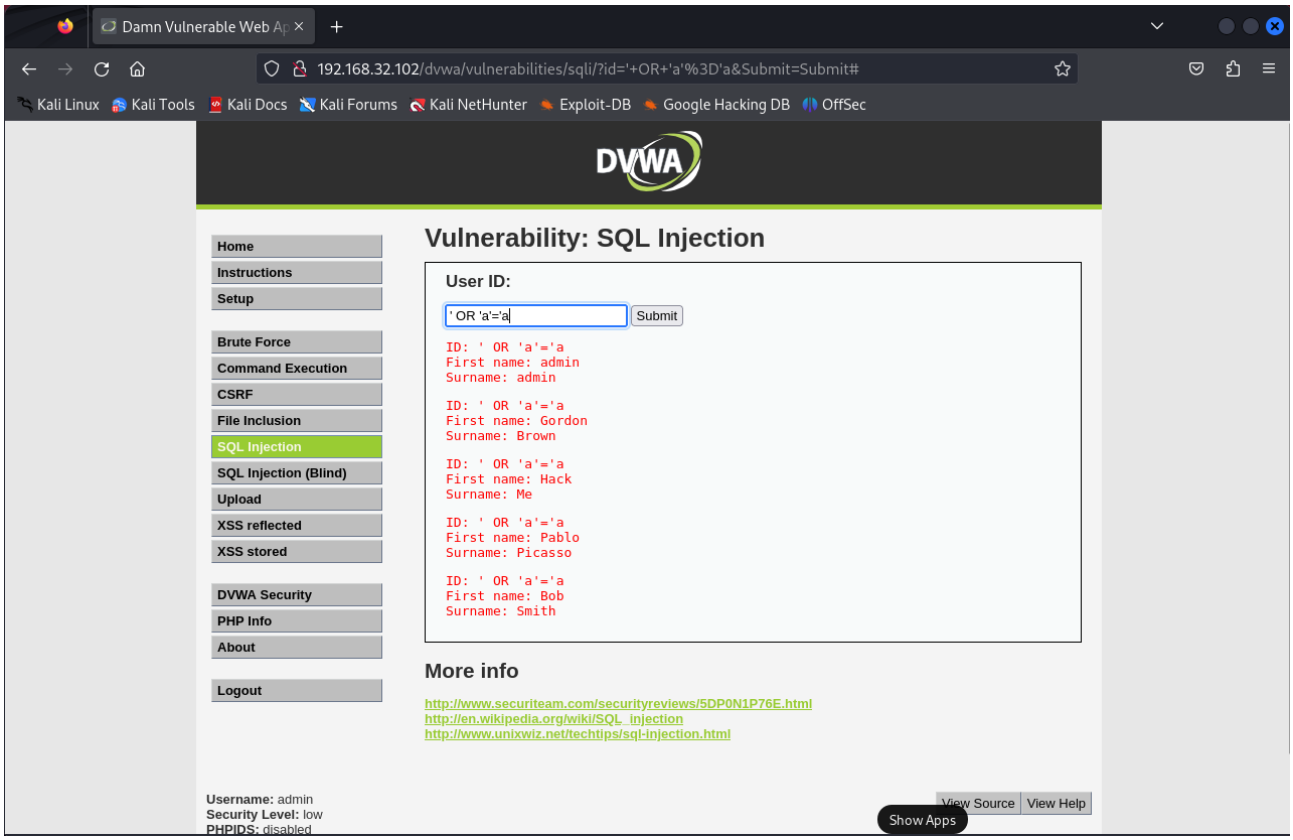


Si noti lo script utilizzato riportato nell’URL della pagina.

Sfruttamento della Vulnerabilità SQL Injection

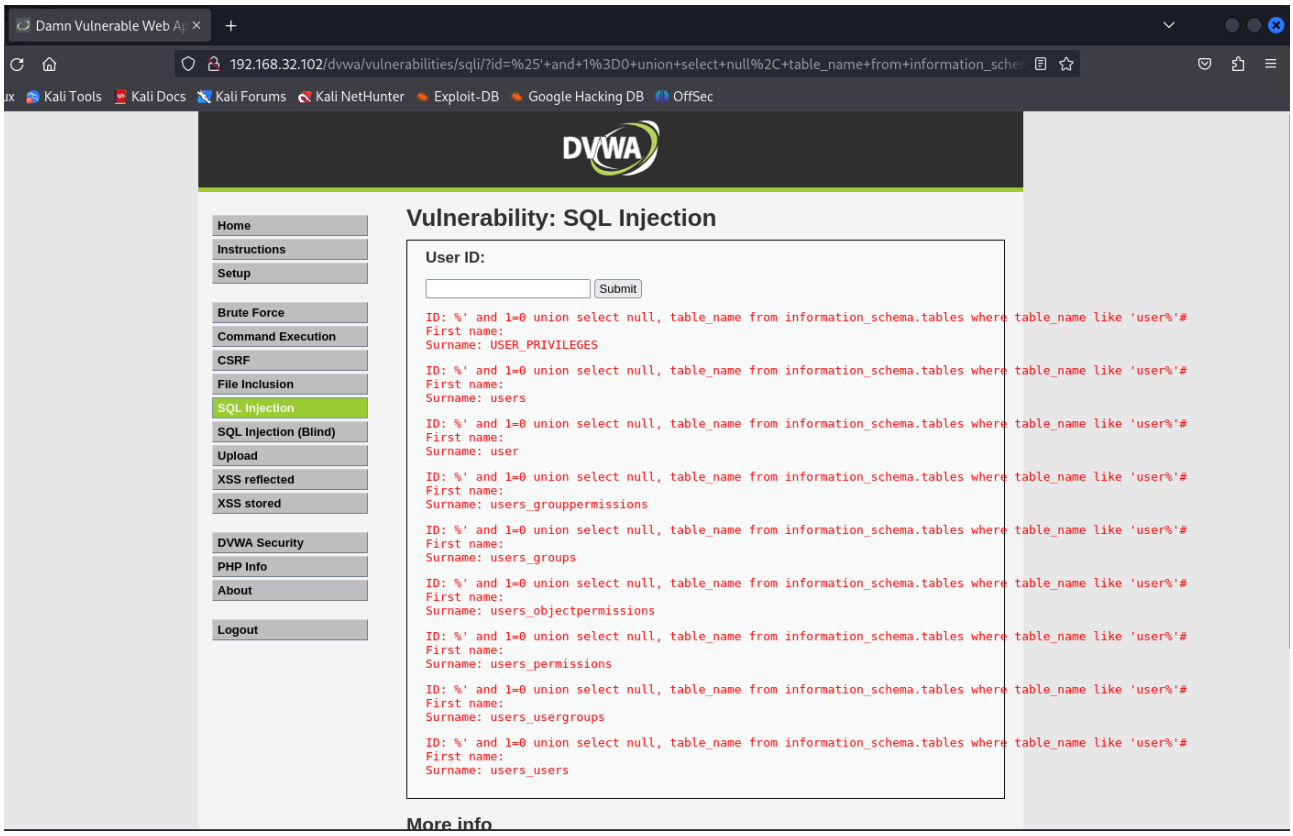
In baso a quanto abbiamo appreso a lezione ed Identificato un input vulnerabile all'interno della DVWA è stato utilizzato per l'esecuzione di un attacco SQL injection.

La prima tecnica utilizzata per sfruttare con successo la vulnerabilità SQL injection è stata imparata a lezione, abbiamo utilizzato la scritta ‘ OR ‘a’=’a in modo da creare una condizione sempre vera che il database legge per giusta e ci permette l’accesso. In questo caso essendo una scelta generica riguardo gli user_ID del campo di input ci è stato mostrato ad output tutti gli utenti registrati con i rispettivi First_name e Last_name come da screen.



Un'altra dimostrazione di SQL injection è stata fatta utilizzando del codice SQL più complesso ma capace di mostrare ad output tutte le tabelle memorizzate nel database in esame, il comando è: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#

Dimostrazione nel comando come da screen.



Conclusioni

In conclusione, il laboratorio di vulnerabilità è stato un'esperienza istruttiva, mettendo in luce la criticità delle minacce informatiche. L'attuazione di attacchi XSS e SQL injection sulla DVWA ha evidenziato l'importanza di implementare solide pratiche di sicurezza. Questa simulazione pratica ha fornito una comprensione più approfondita delle potenziali vulnerabilità nelle applicazioni web e ha sottolineato la necessità di adottare misure preventive.