L’obiettivo di questo esercizio è configurare un ambiente virtuale che includa **Damn Vulnerable Web Application (DVWA)** e una macchina attaccante con **Kali Linux** per eseguire e analizzare vulnerabilità XSS e SQL Injection. DVWA è un’applicazione web deliberatamente vulnerabile, progettata per testare tecniche di penetration testing. Questo laboratorio permette di comprendere meglio le potenziali debolezze nelle applicazioni web e di sperimentare tecniche di attacco in modo sicuro.

Obiettivi Specifici

1. Configurare l’ambiente virtuale e verificare la connessione tra Kali Linux e DVWA.
2. Accedere a DVWA e impostare il livello di sicurezza su **LOW**.
3. Sfruttare una vulnerabilità di **Cross-Site Scripting (XSS) reflected**.
4. Sfruttare una vulnerabilità di **SQL Injection non blind**.

Attacco Cross-Site Scripting (XSS) Reflected

Descrizione della Vulnerabilità

Una vulnerabilità **XSS reflected** permette di iniettare codice JavaScript che viene riflesso (cioè rispedito all'utente) senza essere filtrato o convalidato. Questo tipo di attacco può portare al furto di cookie, alla manipolazione della sessione o all’esecuzione di altre azioni dannose sul client.

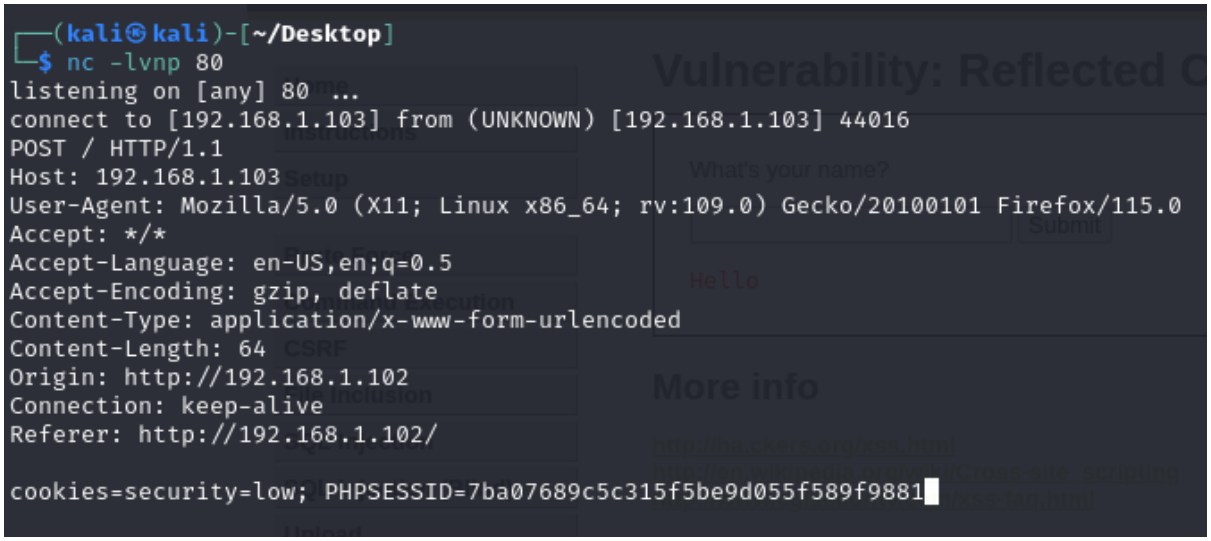
Passi per Sfruttare la Vulnerabilità

1. Ho navigato fino alla sezione vulnerabile XSS Reflected in DVWA
2. Nel campo di input, ho inserito uno script dannoso

Analisi dei Risultati

L’attacco XSS reflected è stato eseguito con successo, dimostrando che DVWA accetta e visualizza il contenuto dell’input senza filtrarlo. Questo rende possibile l'esecuzione di codice JavaScript malevolo nel contesto del browser dell’utente.

Per verificare i risultati abbiamo utilizzato netcat su kali

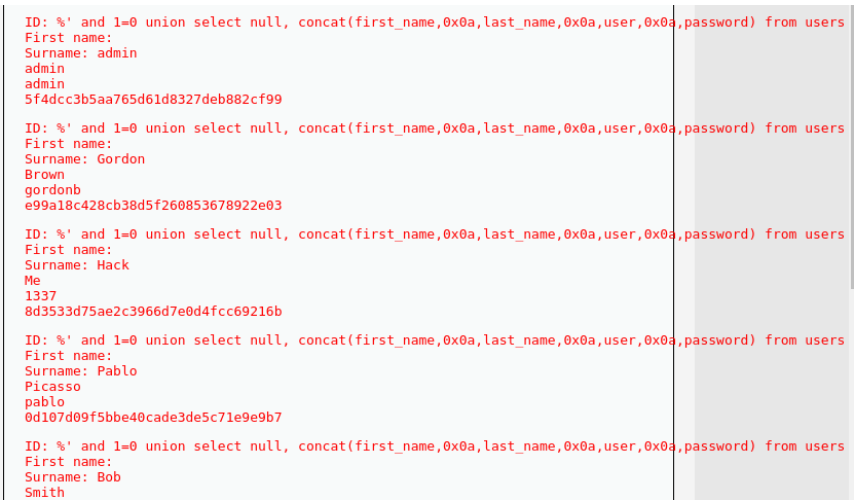


SQL INJECTION

Descrizione della Vulnerabilità

Una **SQL Injection non blind** permette a un attaccante di manipolare query SQL inviate al database attraverso input non sanitizzato. Questo tipo di vulnerabilità consente di estrarre informazioni dal database direttamente nelle risposte dell'applicazione.

Per questo esercizio abbiamo cercato un codice che ci mostrasse più dati, comepresi username e password



Le password verranno mostrate in codice hash

Il codice utilizzato è il seguente: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users

Una vulnerabilità SQL Injection non blind può consentire a un attaccante di ottenere l'accesso a dati sensibili.

Gli attacchi XSS e SQL injection eseguiti su DVWA hanno dimostrato come le applicazioni vulnerabili possano esporre dati sensibili e permettere l'esecuzione di codice non autorizzato.