Report di Sfruttamento delle Vulnerabilità in DVWA

Traccia

Configurate il vostro laboratorio virtuale per raggiungere la DVWA dalla macchina Kali Linux (l'attaccante). Assicuratevi che ci sia comunicazione tra le due macchine con il comando ping.

Raggiungete la DVWA e settate il livello di sicurezza a 'LOW'. Scegliete una delle vulnerabilità XSS ed una delle vulnerabilità SQL Injection: lo scopo del laboratorio è sfruttare con successo le vulnerabilità con le tecniche viste nella lezione teorica.

La soluzione riporta l'approccio utilizzato per le seguenti vulnerabilità:
- XSS reflected.
- SQL Injection (non blind).

Obiettivo

L'obiettivo del laboratorio è configurare un ambiente virtuale per raggiungere DVWA dalla macchina Kali Linux (attaccante), assicurarsi che ci sia comunicazione tra le due macchine, e sfruttare con successo le vulnerabilità XSS reflected e SQL Injection (non blind) con le tecniche viste nella lezione di stamattina.

Accesso a DVWA e Configurazione della Sicurezza

1. Aprire un browser sulla macchina Kali e accedere a DVWA utilizzando l'indirizzo IP della macchina DVWA.
2. Effettuare il login con le credenziali predefinite.
3. Settare il livello di sicurezza a 'LOW'.

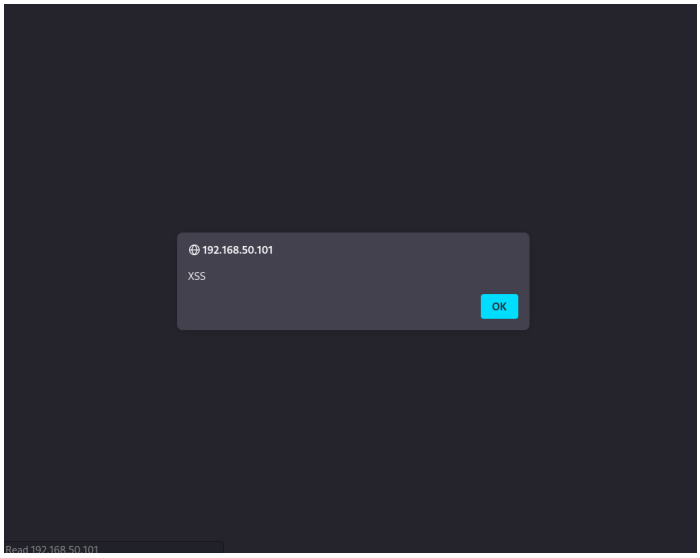
Sfruttamento delle Vulnerabilità

1. XSS Reflected

Descrizione della Vulnerabilità:
La vulnerabilità XSS (Cross-Site Scripting) reflected si verifica quando un'applicazione web prende un dato fornito dall'utente e lo riflette immediatamente in una risposta senza una corretta validazione o codifica. Questo permette agli attaccanti di iniettare codice JavaScript malevolo che verrà eseguito nel contesto del browser della vittima.

Approccio Utilizzato:
1. Navigare alla pagina 'XSS (Reflected)' su DVWA.
2. Inserire il seguente payload nel campo di input:
   <script>alert('XSS');</script>
3. Submettere il modulo.
4. Verificare che venga visualizzato un alert con il messaggio 'XSS'.

Risultati Ottenuti:
L'iniezione del payload ha avuto successo e il codice JavaScript è stato eseguito nel contesto del browser, visualizzando l'alert con il messaggio 'XSS'.

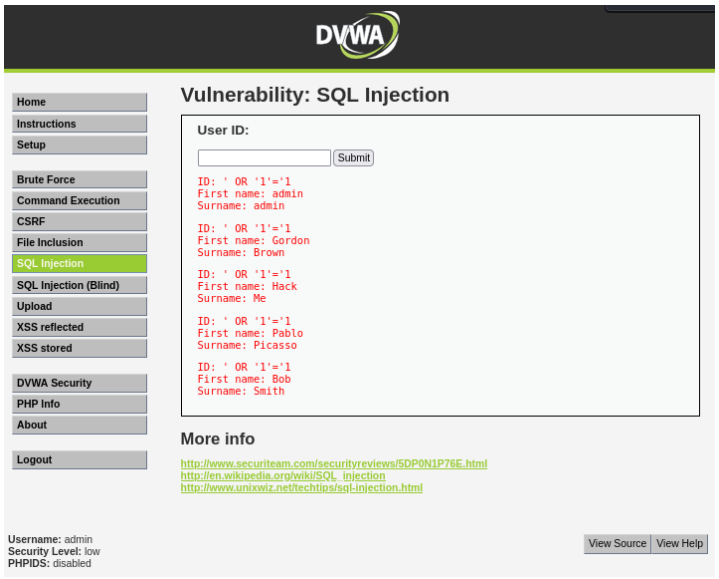


2. SQL Injection (Non Blind)

Descrizione della Vulnerabilità:
La vulnerabilità SQL Injection si verifica quando un'applicazione permette agli utenti di fornire input non validati che vengono poi utilizzati nelle query SQL. Ciò può permettere agli attaccanti di eseguire comandi SQL arbitrari, esfiltrare dati sensibili o manipolare il database.

Approccio Utilizzato:
1. Navigare alla pagina 'SQL Injection' su DVWA.
2. Inserire il seguente payload nel campo di input:
   ' OR '1'='1
3. Submettere il modulo.
4. Verificare che vengano restituiti tutti i record dal database.

Risultati Ottenuti:
L'iniezione del payload ha avuto successo e la query SQL è stata manipolata per restituire tutti i record del database, mostrando che l'applicazione è vulnerabile a SQL Injection.



Le vulnerabilità XSS reflected e SQL Injection sono state sfruttate con successo seguendo i passi descritti.