Report Finale: Sfruttamento di Vulnerabilità su DVWA

Introduzione

In questo esercizio, abbiamo configurato un laboratorio virtuale per esplorare le vulnerabilità di sicurezza web utilizzando Damn Vulnerable Web Application (DVWA) e Kali Linux. L'obiettivo è stato quello di sfruttare con successo una vulnerabilità XSS reflected e una vulnerabilità SQL Injection non blind. Questo report descrive l'approccio utilizzato per identificare e sfruttare queste vulnerabilità.

Ambiente di Test

- **Macchina Attaccante:** Kali Linux
- **Macchina Target:** DVWA (Damn Vulnerable Web Application) eseguito su una macchina virtuale Ubuntu

Le macchine virtuali sono state configurate sulla stessa rete virtuale per garantire la comunicazione tra di loro.

1. XSS Reflected

Descrizione della Vulnerabilità

L'XSS Reflected (Cross-Site Scripting) è una vulnerabilità che consente a un attaccante di iniettare codice JavaScript malevolo che viene eseguito nel contesto del browser della vittima. Questo tipo di vulnerabilità si verifica quando l'applicazione riflette l'input dell'utente senza una corretta sanitizzazione.

Approccio Utilizzato

1. **Accesso a DVWA:**
   - Navigato su http://[IP_DVWA]/dvwa dalla macchina Kali Linux.
   - Effettuato il login con le credenziali predefinite (username: admin, password: password).
2. **Settaggio del Livello di Sicurezza:**
   - Impostato il livello di sicurezza su "LOW" nella sezione "DVWA Security".
3. **Identificazione della Vulnerabilità:**
   - Navigato alla sezione "XSS (Reflected)".
   - Inserito il seguente script nel campo di input:
   - html
   - Copia codice
   - <script>alert('XSS');</script>
4. **Esecuzione dell'Attacco:**

- Cliccato su "Submit" e verificato che un popup di alert con il messaggio "XSS" venisse eseguito.

Risultato

Il popup di alert è stato visualizzato correttamente, confermando che la vulnerabilità XSS reflected è presente e può essere sfruttata per eseguire codice JavaScript arbitrario.

2. SQL Injection

Descrizione della Vulnerabilità

La SQL Injection è una vulnerabilità che consente a un attaccante di interferire con le query SQL eseguite dall'applicazione. La variante non blind permette di ottenere direttamente i risultati della query manipolata, esponendo potenzialmente informazioni sensibili del database.

Approccio Utilizzato

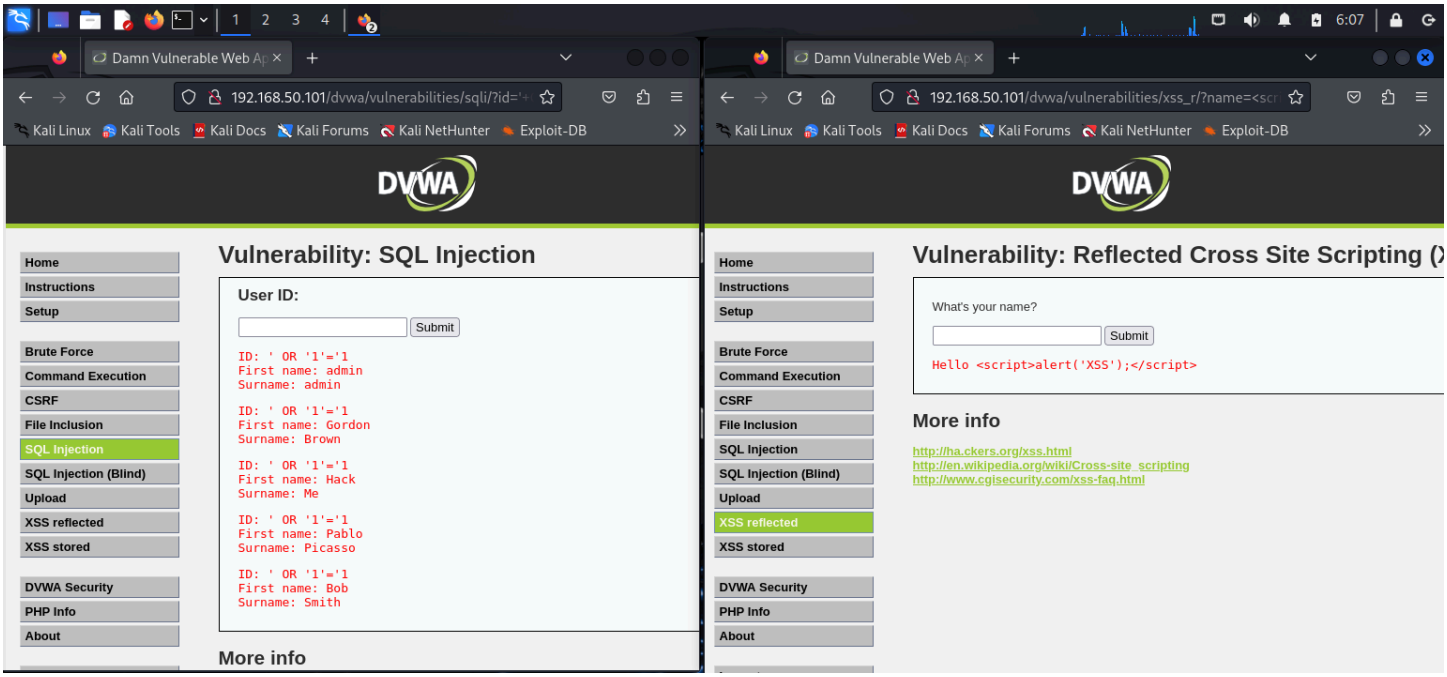
1. **Accesso a DVWA:**
   - Navigato su http://[IP_DVWA]/dvwa dalla macchina Kali Linux.
   - Effettuato il login con le credenziali predefinite (username: admin, password: password).
2. **Settaggio del Livello di Sicurezza:**
   - Impostato il livello di sicurezza su "LOW" nella sezione "DVWA Security".
3. **Identificazione della Vulnerabilità:**
   - Navigato alla sezione "SQL Injection".
   - Inserito il seguente payload nel campo ID:
   - sql
   - Copia codice
   - ' OR '1'='1
4. **Esecuzione dell'Attacco:**
   - Cliccato su "Submit" e osservato i risultati. La query SQL manipolata ha restituito tutti i record della tabella utenti, mostrando informazioni di più utenti.

Risultato

I risultati mostrati dopo l'iniezione hanno confermato che la query SQL è stata manipolata con successo, esponendo dati che normalmente non sarebbero stati accessibili.

Conclusioni

Entrambe le vulnerabilità sono state sfruttate con successo, dimostrando come l'input non sanitizzato possa portare a seri rischi di sicurezza.



- **XSS Reflected:** Permette l'esecuzione di codice JavaScript arbitrario nel contesto del browser della vittima.
- **SQL Injection:** Consente l'accesso non autorizzato ai dati del database.

Mitigazioni

Per prevenire tali vulnerabilità, si raccomandano le seguenti pratiche di sicurezza:

- **Sanitizzazione dell'Input:** Utilizzare funzioni di escaping e sanitizzazione per tutti gli input degli utenti.
- **Prepared Statements:** Utilizzare query parametrizzate per prevenire SQL Injection.
- **Validazione dei Dati:** Implementare una robusta validazione lato server per tutti gli input.
- **CSP (Content Security Policy):** Implementare politiche di sicurezza dei contenuti per mitigare XSS.