27 FEBBRAIO 2024

REPORT - EPICODE

S6L2

PRESENTED BY

Alessandro Marasca

EXPLOIT DVWA - XSS E SQL INJECTION

Traccia

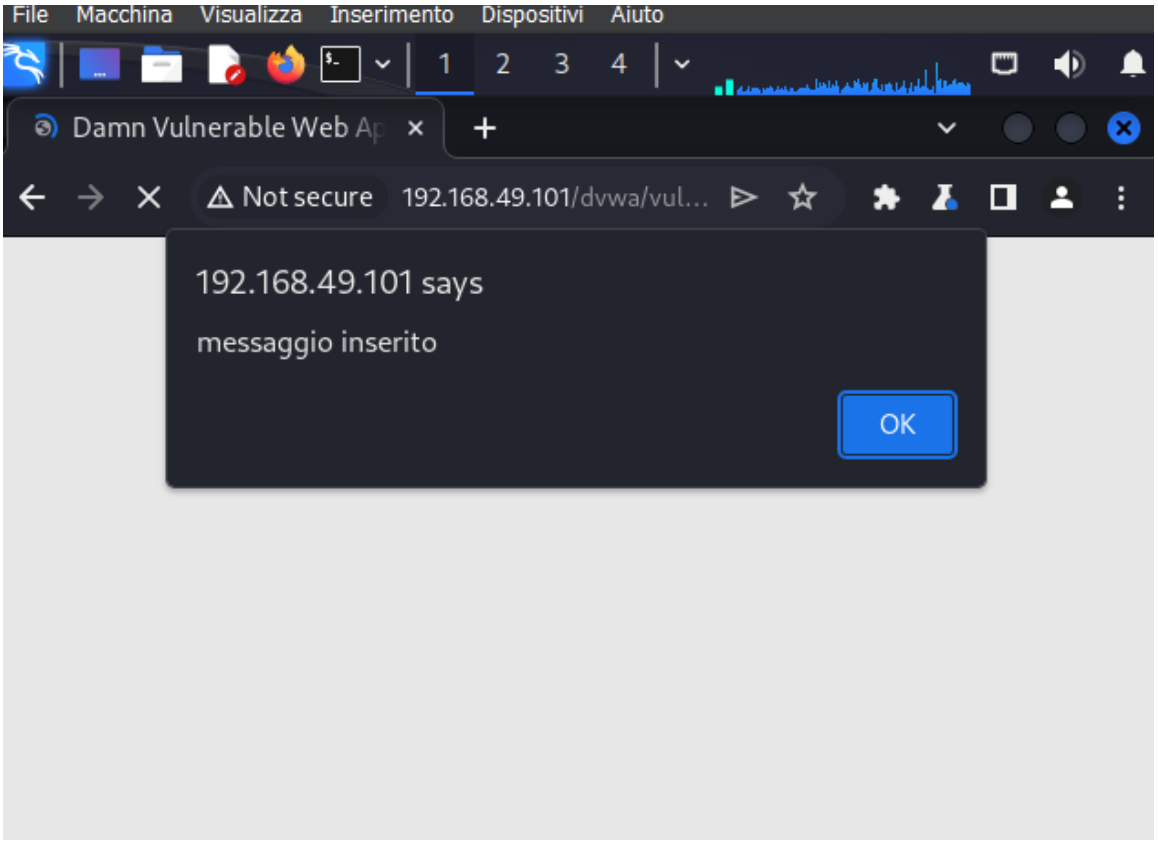
Configurate il vostro laboratorio virtuale per raggiungere la DVWA dalla macchina Kali Linux (l'attaccante).
Assicuratevi che ci sia comunicazione tra le due macchine con il comando ping.

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:

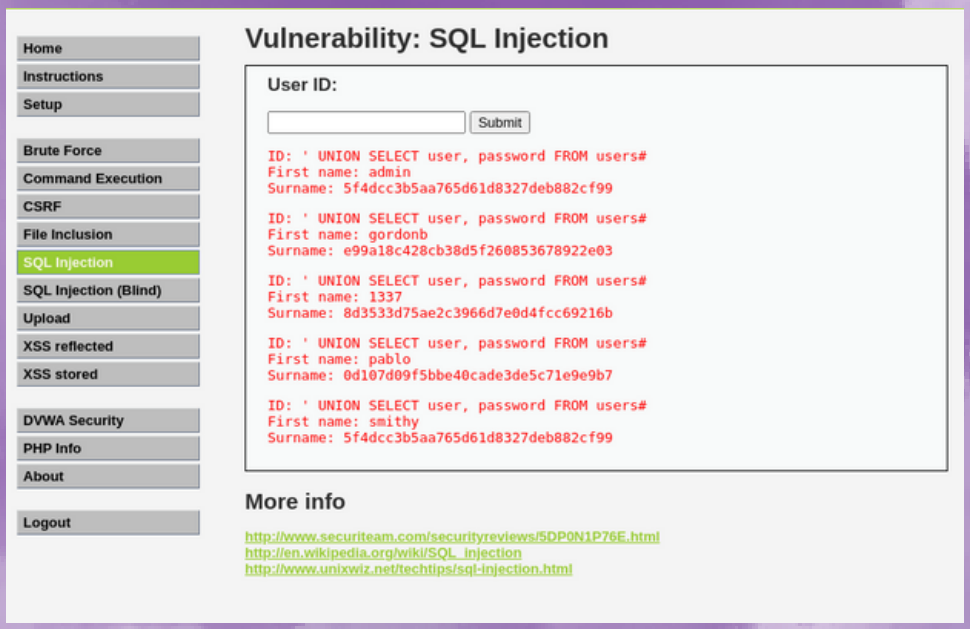
- **XSS reflected**
- **SQL Injection (non blind)**

XSS REFLECTED



Notiamo come impostando la sicurezza della DVWA di Metasploitable 2 su “Low” sia semplice inserire l’XSS. Inserendo lo script **<script>alert(“messaggio inserito”)</script>**

SQL INJECTION (NON BLIND)



Alessandro Marasca

Epicode

S6L2- CS0124

27 FEBBRAIO 2024