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**)

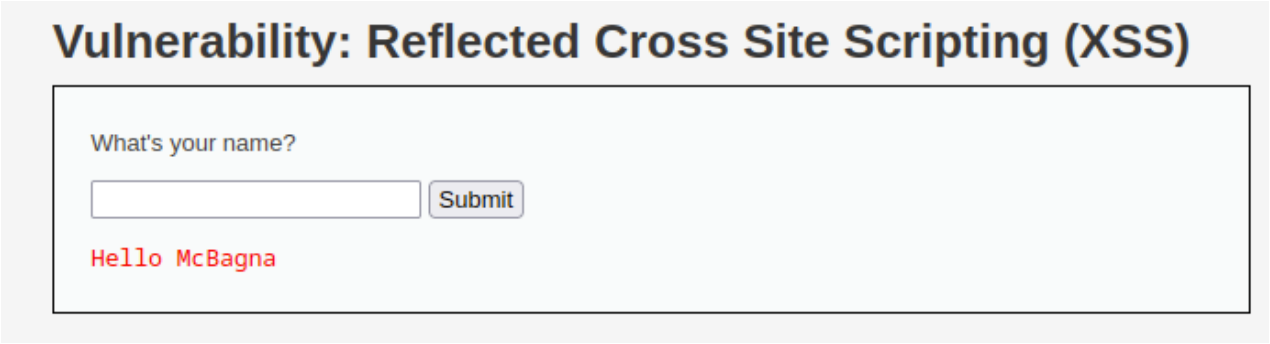
Consegna:

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

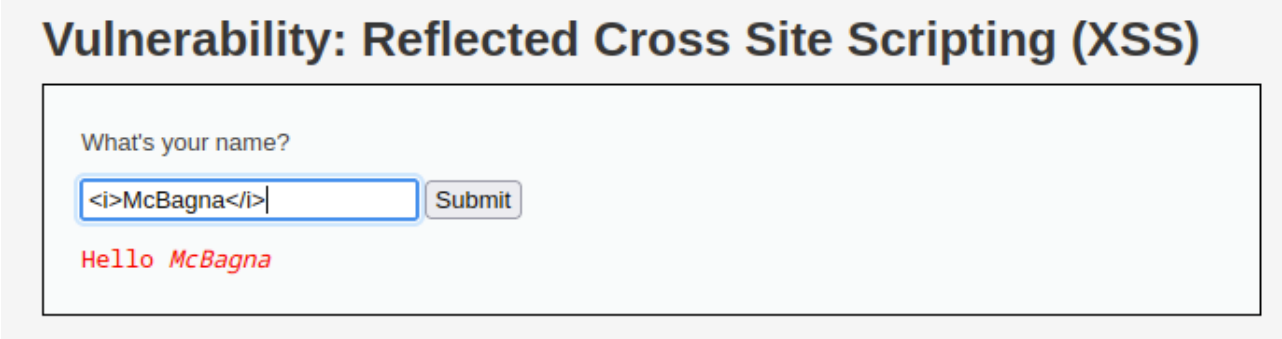
SQL
1. Controllo di injection
2. Esempi
3. Union Screenshot/spiegazione in un report di PDF

Svolgimento:

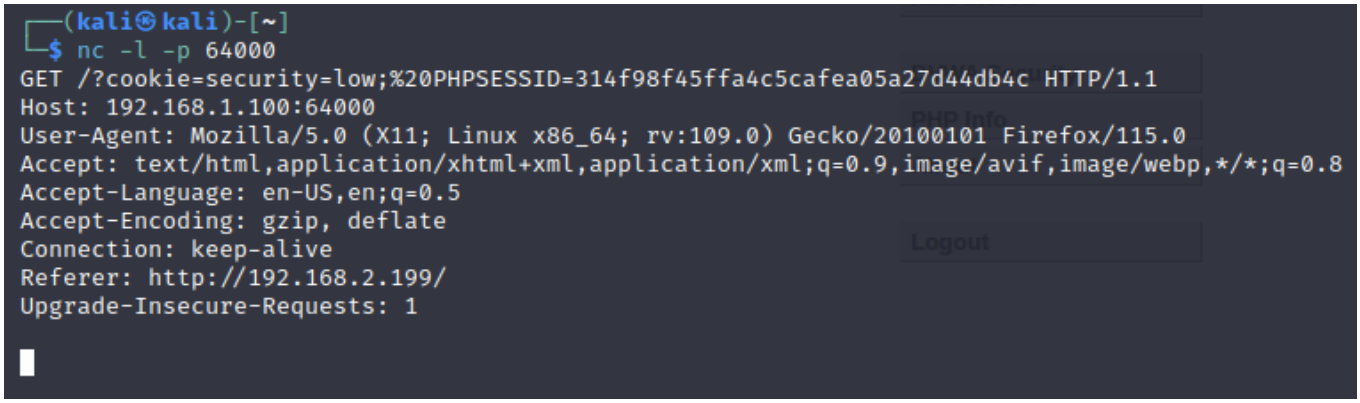
Inserimento del solo testo con relativo output



Inserimento del testo con aggiunta elemento di scripting per il corsivo



Inserimento dello script per catturare i cookie lasciando una netcat in ascolto su una porta a scelta



Tramite SQL Injection con una condizione sempre vera ci facciamo restituire gli username e gli hash delle rispettive password