

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».

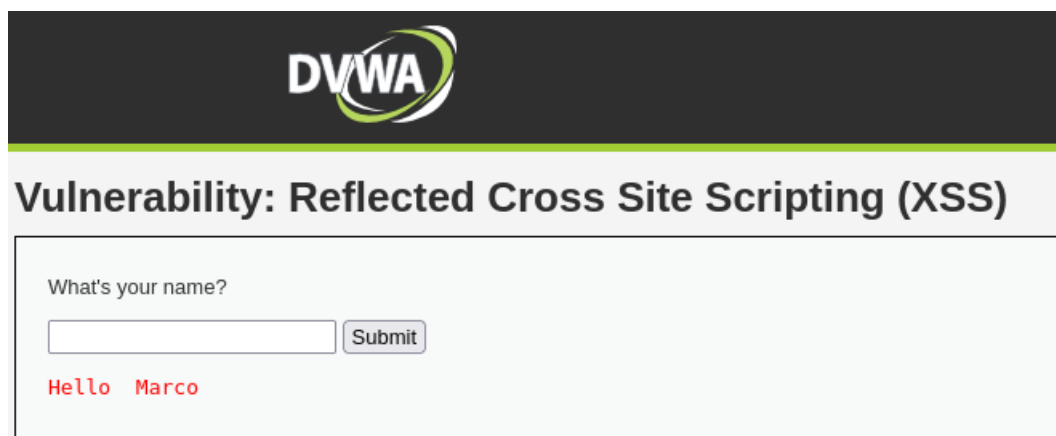
Scegliete una delle vulnerabilità XSS ed una delle vulnerabilità SQL injection: lo scopo del laboratorio è sfruttare con successo le vulnerabilità con le tecniche viste nella lezione teorica.

La soluzione riporta l'approccio utilizzato per le seguenti vulnerabilità:

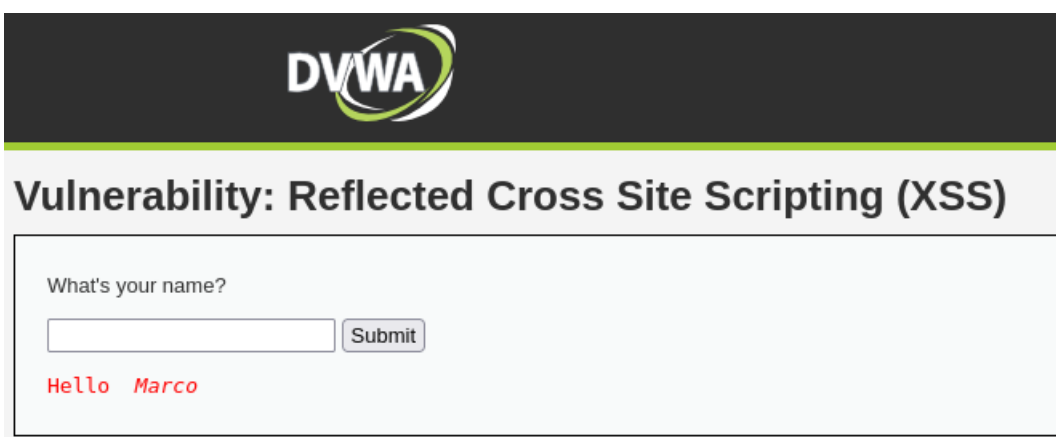
- XSS reflected
- SQL Injection (non blind)

Nell'esercizio di oggi sono andato a sfruttare due vulnerabilità della DVWA di Metasploitable tramite attacchi XSS e SQL injection.

Per prima cosa sono entrato nella DVWA, nella parte relativa agli XSS reflected. Ho testato la pagina per confermare che eseguisse del codice, inserendo il mio nome scritto normalmente e in corsivo.

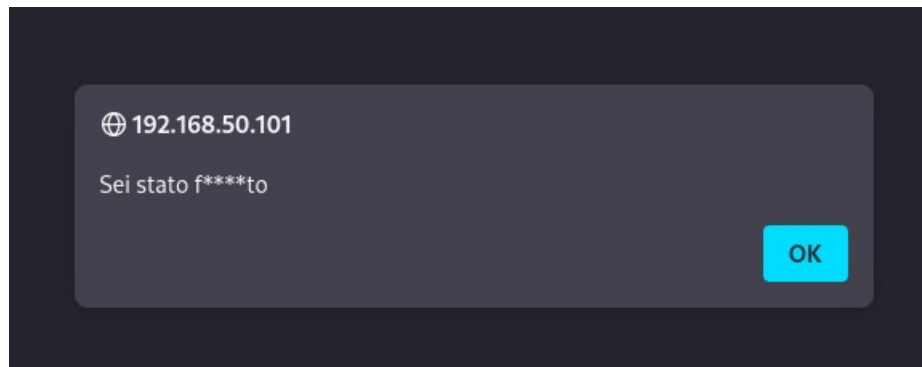


The screenshot shows the DVWA interface with the title "Vulnerability: Reflected Cross Site Scripting (XSS)". Below the title is a form with the label "What's your name?". The input field contains the text "Marco" and the "Submit" button is visible. Below the form, the output "Hello Marco" is displayed in red text.



The screenshot shows the DVWA interface with the title "Vulnerability: Reflected Cross Site Scripting (XSS)". Below the title is a form with the label "What's your name?". The input field contains the text "Marco" in a red, italicized font, and the "Submit" button is visible. Below the form, the output "Hello Marco" is displayed in red text.

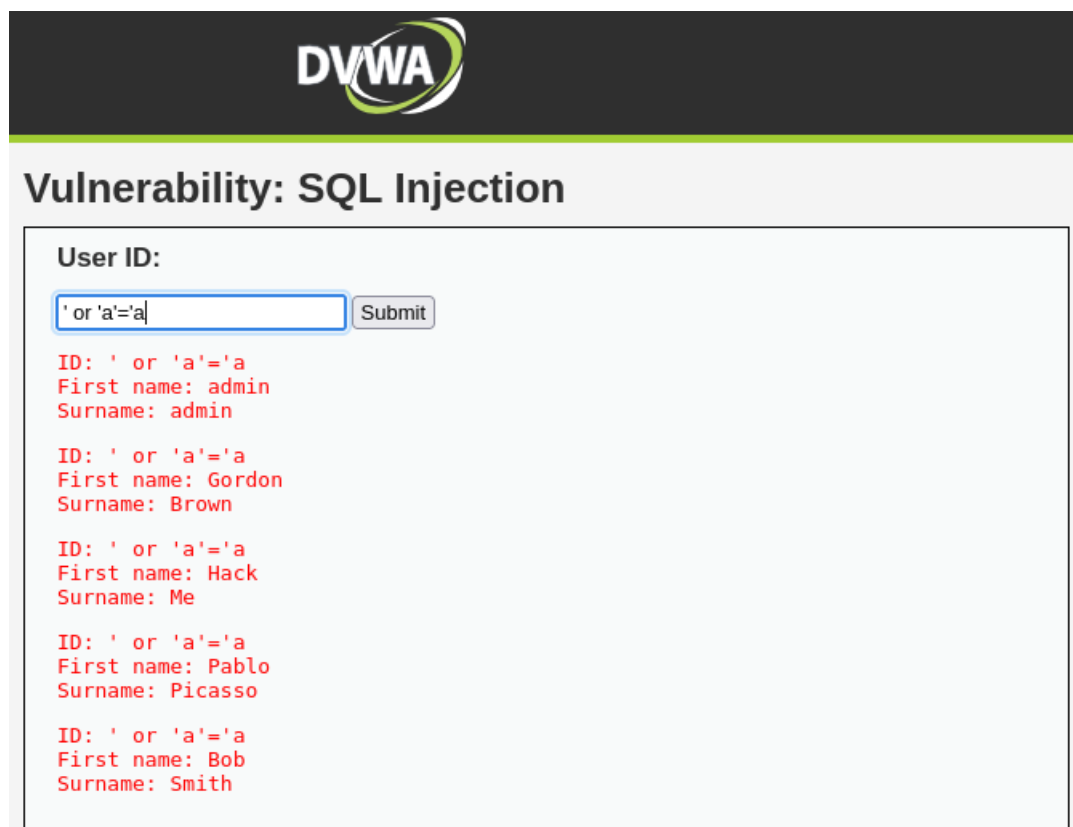
Ho quindi inserito lo script “malevolo” per sfruttare tale vulnerabilità.



Ho testato l'url che risulta inviandolo alla mail personale come link a cui accedere.



Il secondo attacco è un SQL injection, cioè una penetrazione del database back end di un server.



Usando una sintassi che ci dia un ritorno sempre vero possiamo sfruttare la vulnerabilità per accedere a tutti gli utenti del database.