SQL INJECTION
S6L2

Esercizio del Giorno Esercizio Traccia Argomento:

Sfruttamento delle Vulnerabilità XSS e SQL Injection sulla DVWA Obiettivi: Configurare il laboratorio virtuale per sfruttare con successo le vulnerabilità XSS e SQL Injection sulla Damn Vulnerable Web Application DVWA.

Istruzioni per l'esercizio:

1. Configurazione del Laboratorio:

○ Configurate il vostro ambiente virtuale in modo che la macchina DVWA sia raggiungibile dalla macchina Kali Linux (l'attaccante).

○ Verificate la comunicazione tra le due macchine utilizzando il comando ping.

2. Impostazione della DVWA

○ Accedete alla DVWA dalla macchina Kali Linux tramite il browser.

○ Navigate fino alla pagina di configurazione e settate il livello di sicurezza a LOW.

3.Sfruttamento delle Vulnerabilità:

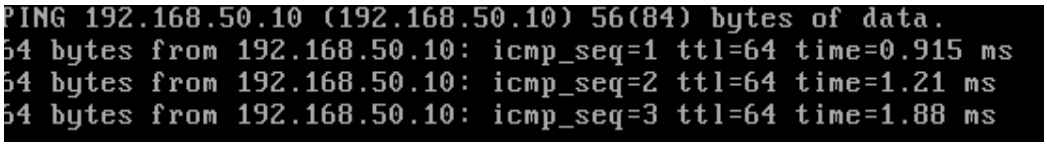
○ Scegliete una vulnerabilità XSS reflected e una vulnerabilità SQL Injection (non blind).

○ Utilizzate le tecniche viste nella lezione teorica per sfruttare con successo entrambe le vulnerabilità.

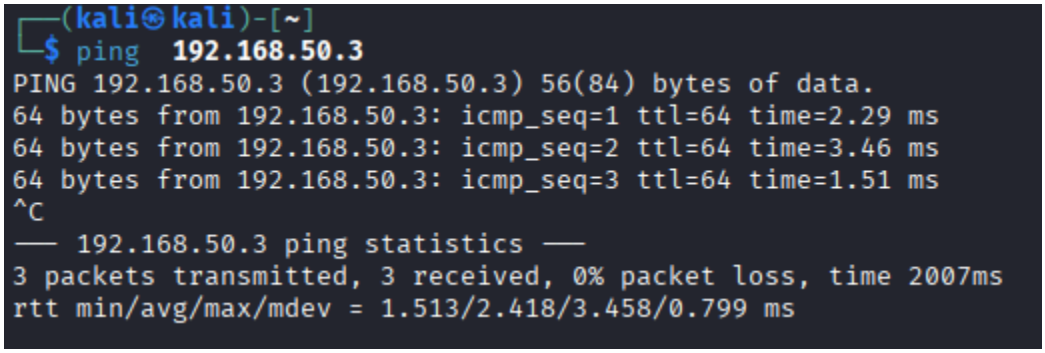
1. Configurazione del laboratorio:

Verifica del collegamento tra le due macchine tramite il comando ping.

Ping da Metasploitable:



Ping da Kali Linux:

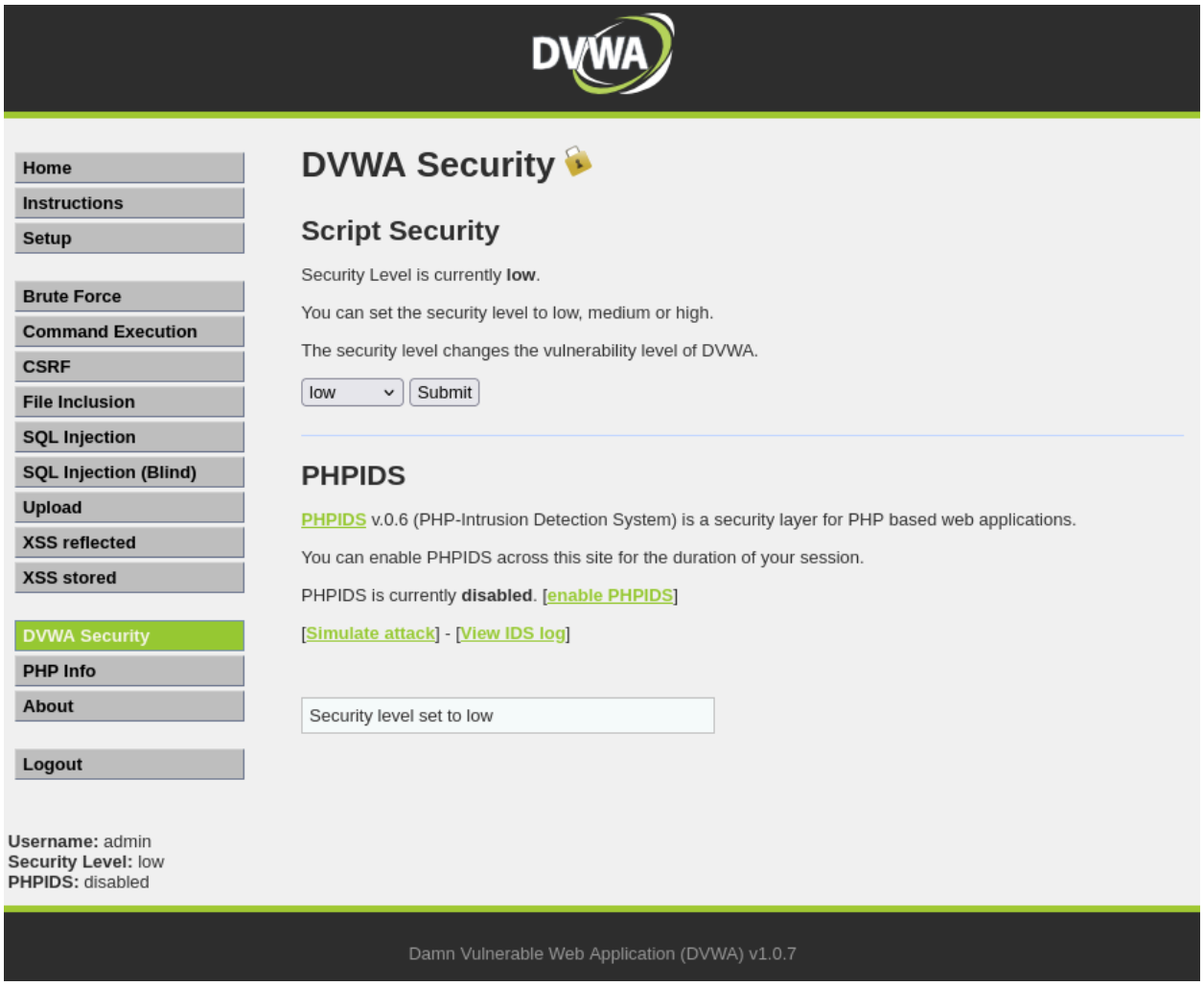


2. Impostazione della DVWA:

Accediamo al browser della Metasploitable sulla macchina virtuale Kali Linux inserendo l'indirizzo IP 192.168.50.3 (Metasploitable) sulla barra di ricerca.

Una volta sulla pagina di metasploitable clicchiamo sul link "DVWA" e accediamo facendo il login con le seguenti credenziali USERNAME="admin" PASSWORD="password"

Una volta fatto l'accesso andiamo su "DVWA Security" e mettiamo il livello di sicurezza su "low" per salvare l'impostazione clicchiamo su "Submit".

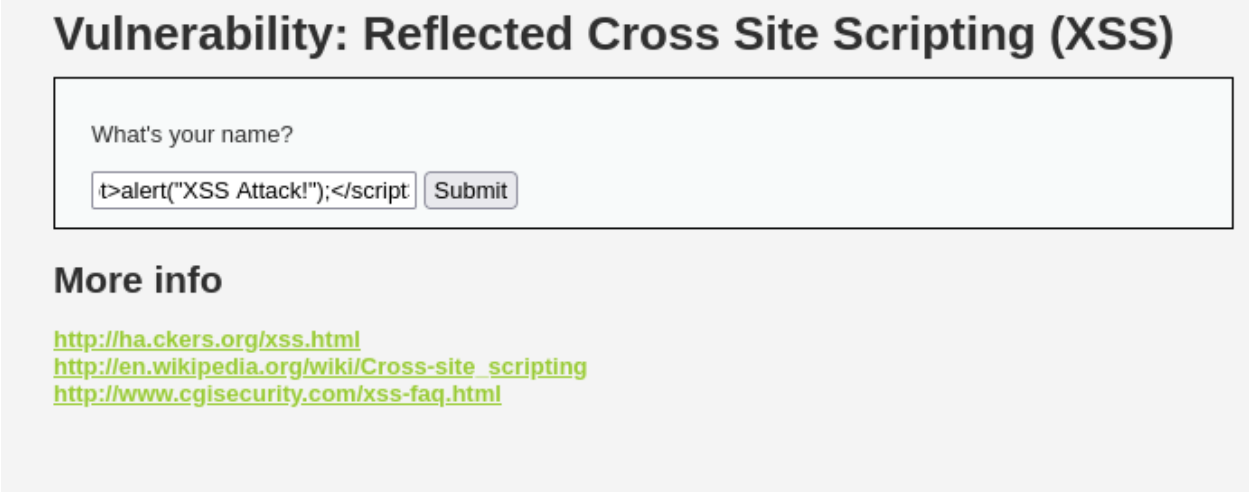


3. Sfruttamento delle vulnerabilità:

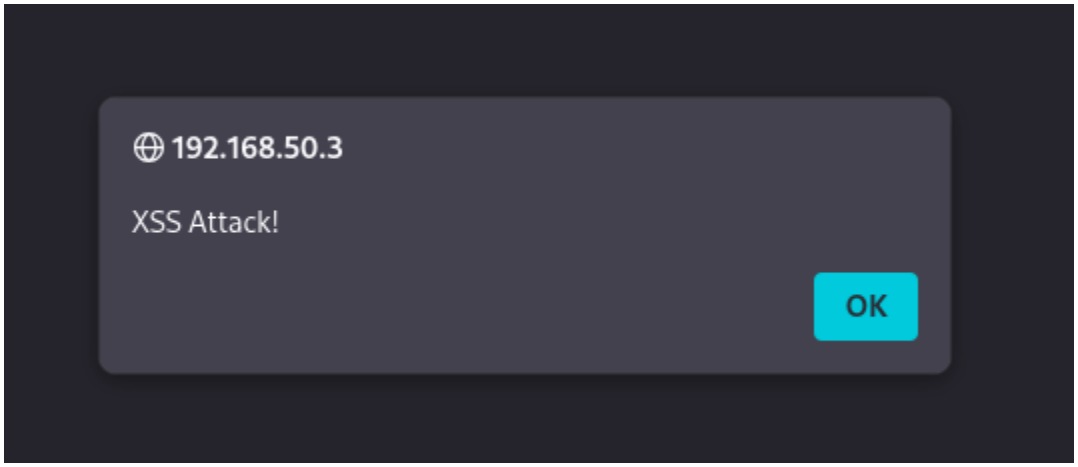
Attacco XSS:

Una volta settato tutto andiamo sulla voce “XSS Reflected” e inseriamo lo script

<script>alert(“XSS Attack!”)</script>



La pagina mostrerà questo popup:



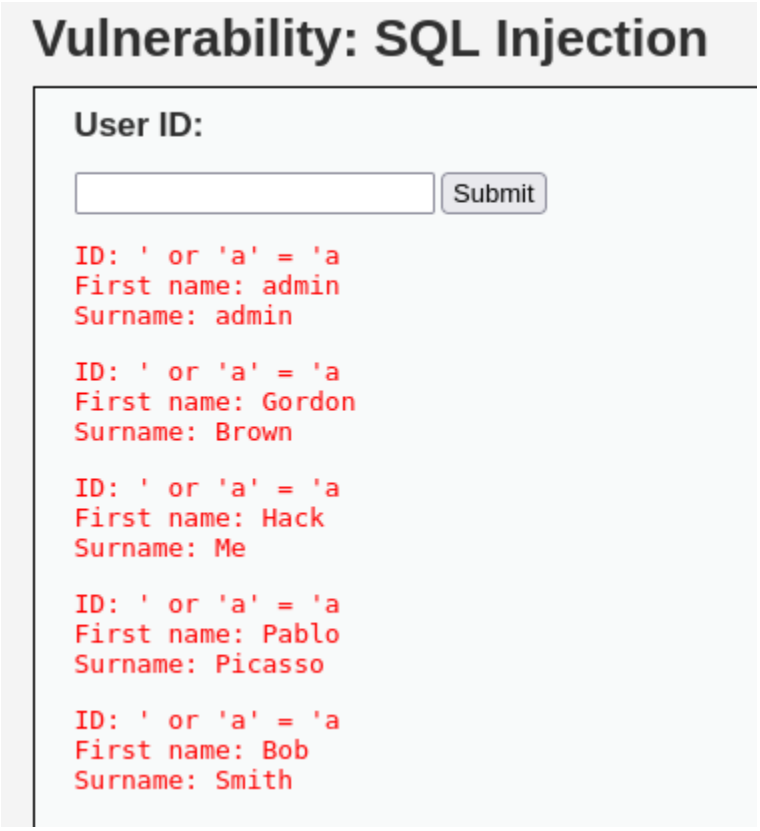
Attacco SQL Injection:

Un attacco di tipo SQL injection permette ad un utente non autorizzato di prendere il controllo sui comandi SQL utilizzati da un'applicazione Web.

Per eseguire un attacco SQL injection su Metasploitable bisogna andare all'omonima voce su DVWA "SQL Injection"

Inseriamo il seguente codice:

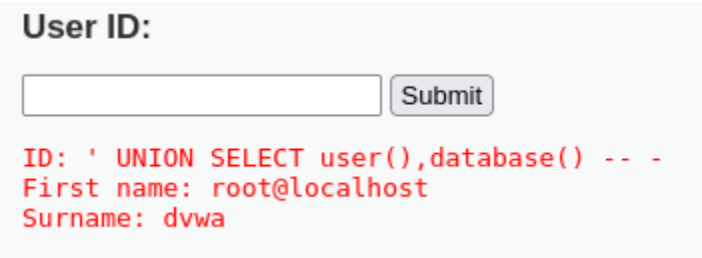
' or 'a' = 'a



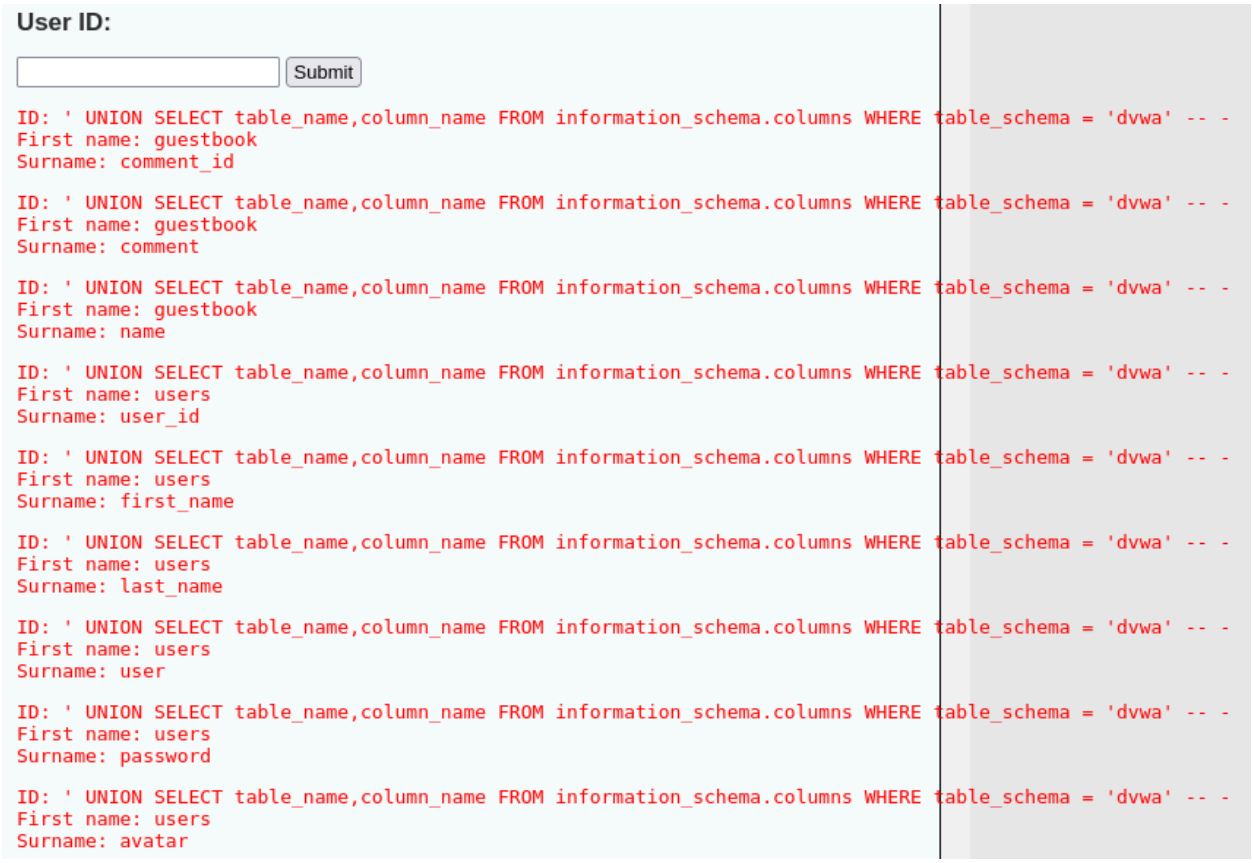
L'OR tra due operandi di cui uno sempre "True" restituisce sempre "True", la query sopra chiede al database di selezionare tutte le entry della tabella Products.

Usiamo il seguente comando:

' UNION SELECT user(),database() -- -



Cerchiamo nel database “DVWA”:



Con il seguente comando ricaviamo username e password degli utenti:

' UNION SELECT user,password FROM dvwa.users -- -