


“RISOLUZIONE ESERCIZIO S6L2”

TRACCIA



Pratica S6/L2 PDF

Esercizio
Traccia

Traccia:

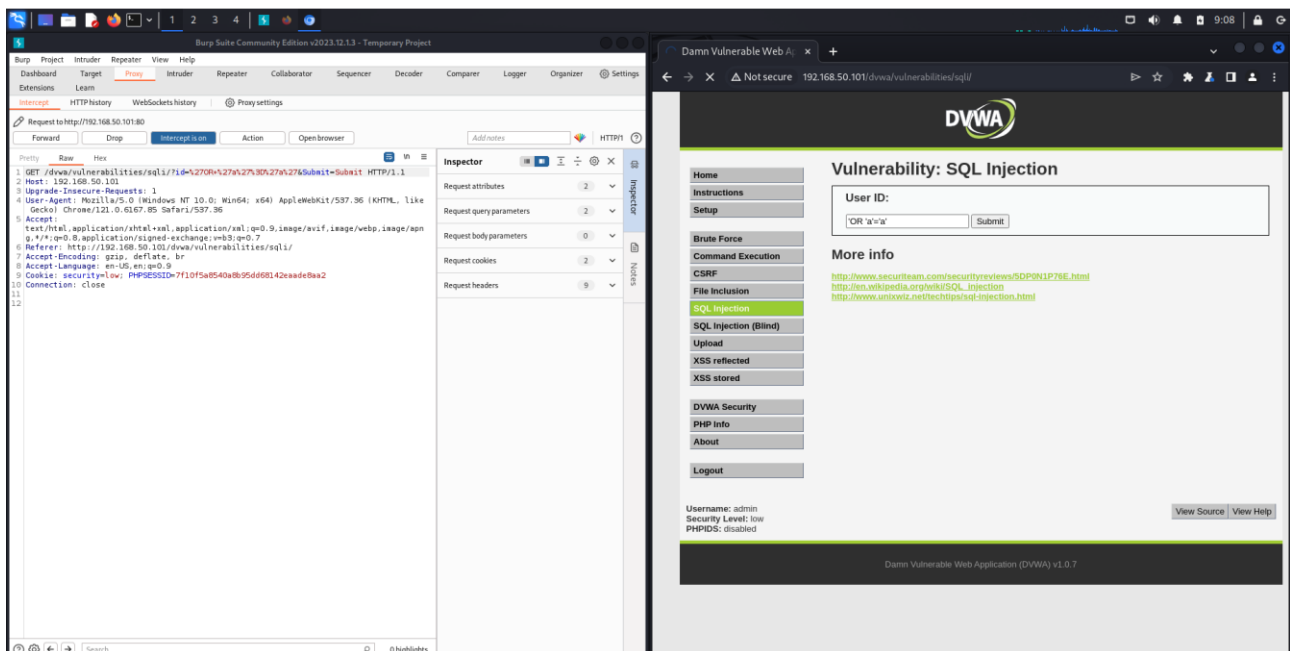
Configurate il vostro laboratorio virtuale per raggiungere la DVWA dalla macchina Kali Linux (l'attaccante). Assicuratevi che ci sia comunicazione tra le due macchine con il comando ping.

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**).

SOLUZIONE PER SQL INJECTION



The screenshot displays the Burp Suite interface on the left and the DVWA web application on the right. In Burp Suite, the HTTP history shows a GET request to `http://192.168.50.101:80/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit`. The Inspector panel shows the request details, including the User-Agent and Accept headers. The DVWA web application shows the 'Vulnerability: SQL Injection' page with a 'User ID' input field and a 'Submit' button. The 'More info' section lists various vulnerabilities, including 'SQL Injection (Blind)' and 'SQL Injection (Reflected)'. The 'Log out' button is visible at the bottom.

ABBIAMO INSERITO IL COMANDO

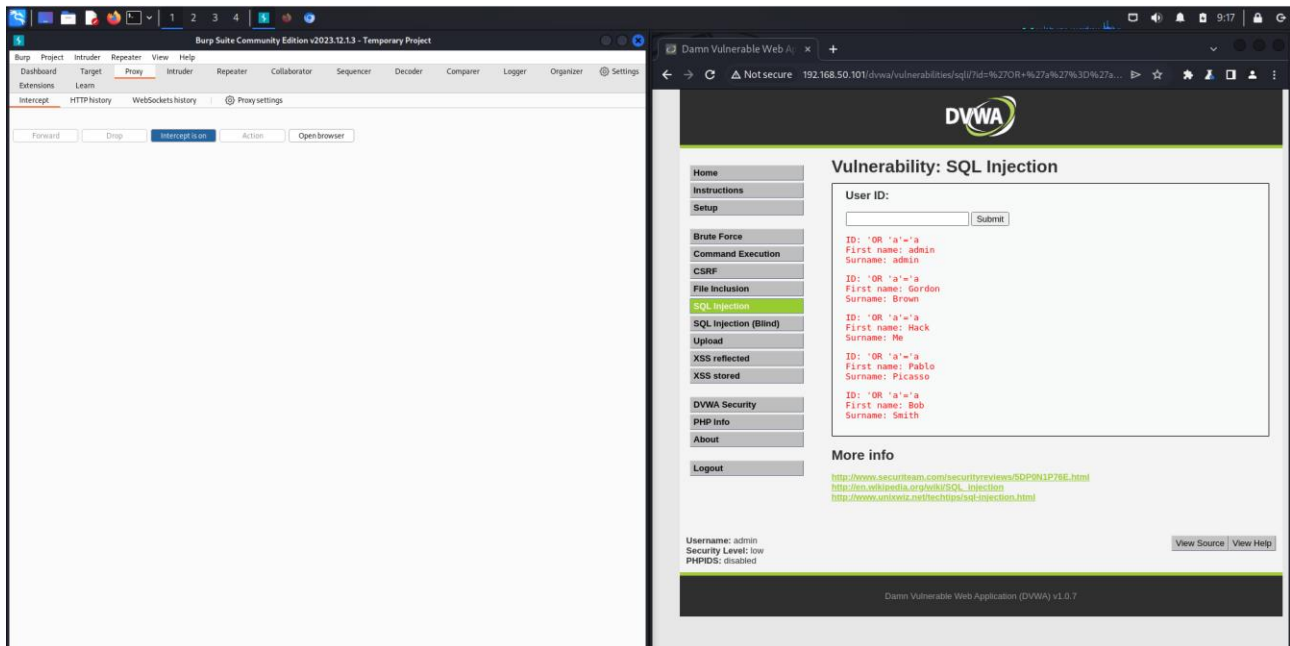
OR 'a' = 'a'

CHE CI FA ACCEDERE ALLA TABELLA PRESENTE SULLA DVWA IN MODO DA VISUALIZZARE I RELATIVI CAMPI :

ID

FIRST NAME

SURNAME



PER PREVENIRE QUESTO ATTACCO POTREMMO INSERIRE UN COMANDO PER FARE IN MODO CHE I CARATTERI SPECIALI VENGANO LETTI COME CARATTERI DI TESTO

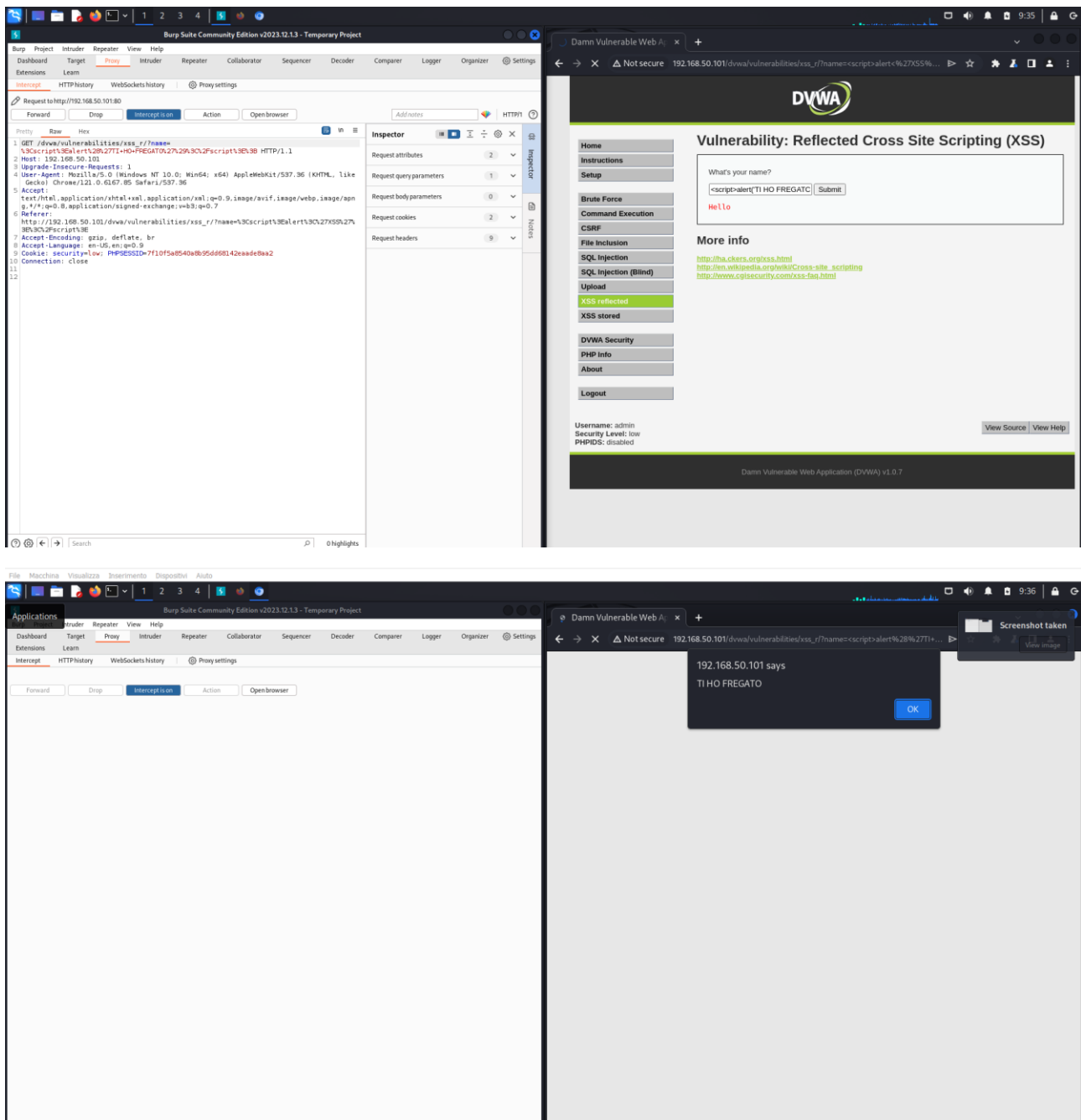
ES.

`$id = $_GET['id'];`

`$id = stripslashes($id);`

`$id = mysql_real_escape_string($id);`

“SOLUZIONE CON XSS REFLECTED”



IN QUESTO CASO ABBIAMO INFETTATO IL PAYLOAD FACENDOGLI APPARIRE UNA RIGA DI TESTO

QUESTO PUO' ESSERE PROTETTO AGGIUNGENDO DEI TOKEN DI SESSIONE OLTRE AI COOKIE.