DVWA — SQL Injection Walkthrough

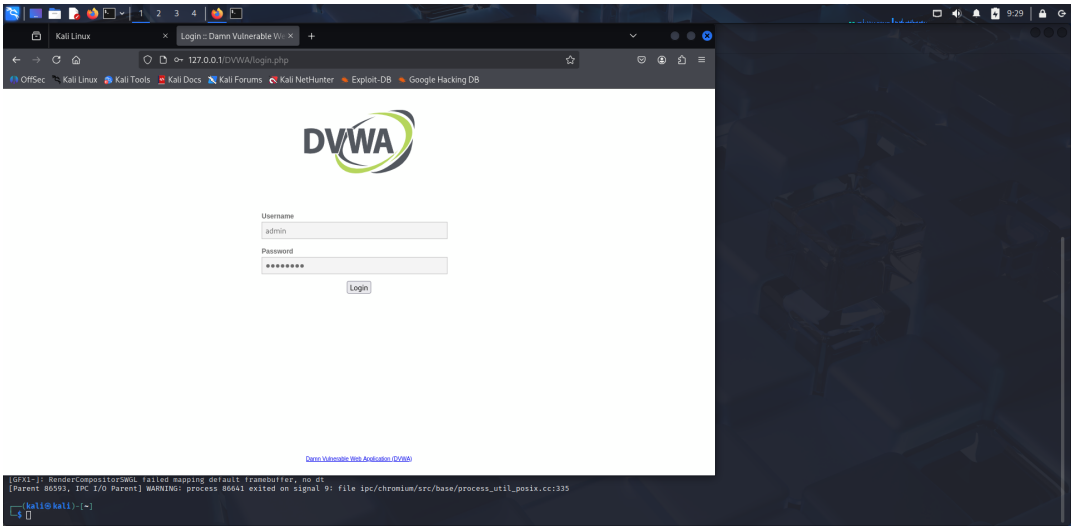
Prepared By: Tarun M
Date: 10/08/2025

Introduction

This document demonstrates a SQL Injection vulnerability test performed on DVWA (Damn Vulnerable Web Application) with security level set to LOW. Screenshots are presented in the correct step-by-step sequence along with explanations.

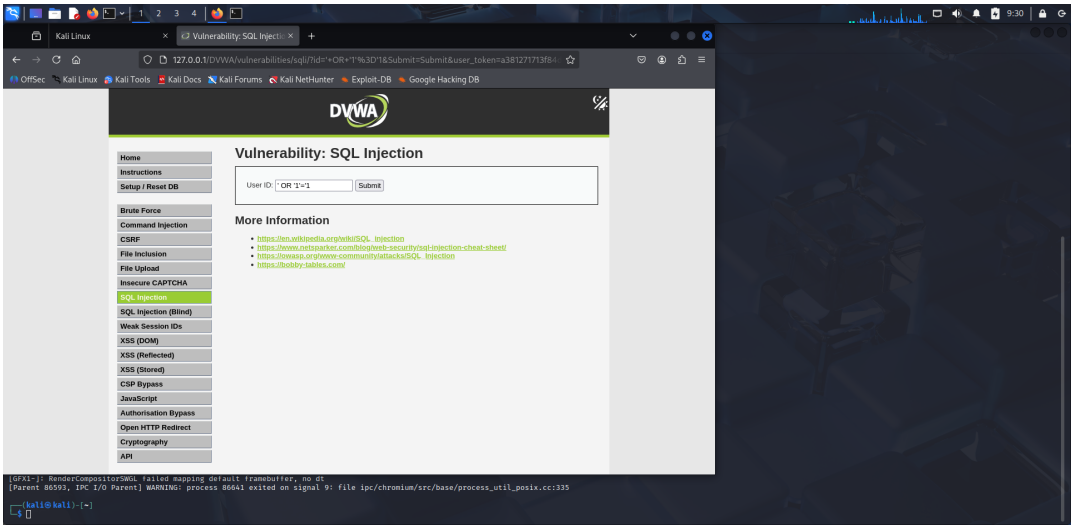
Step 1 — Injection Results

After submitting the payload, the application returned database contents, confirming successful SQL Injection.



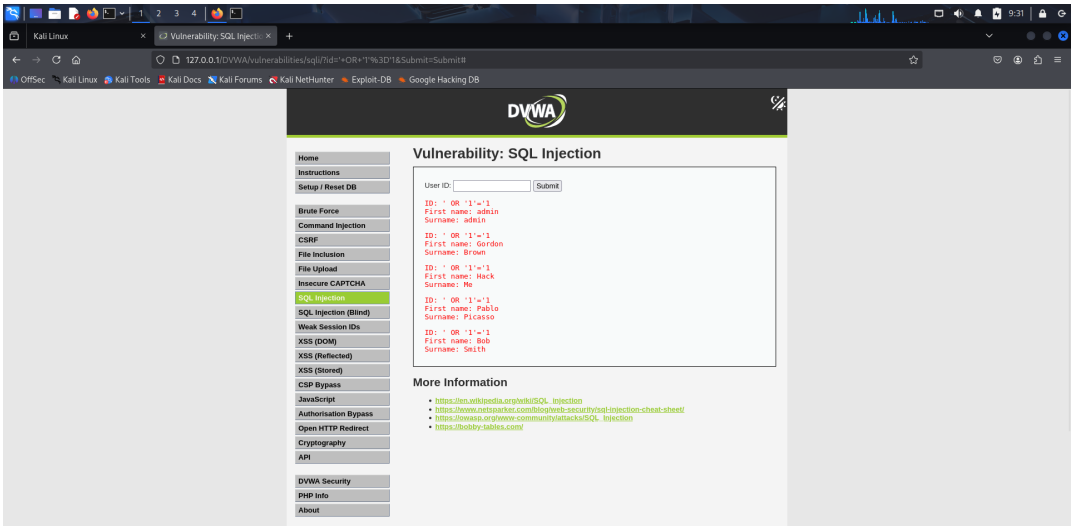
Step 2 — SQL Injection Payload

In the 'SQL Injection' module, the payload ' OR '1'='1 was entered to bypass authentication logic and retrieve all rows.



Step 3 — DVWA Login

Logged into DVWA using default credentials (admin / password) to access the vulnerable modules.



Impact

SQL Injection allows attackers to retrieve sensitive data, bypass authentication, and potentially compromise the entire database.

Mitigation

- Use parameterized queries (prepared statements) - Validate and sanitize all user inputs - Apply least privilege to database accounts - Deploy a Web Application Firewall (WAF) for extra protection