SQL Injection Labs - DVWA (Low, Medium, High)

Introduction

SQL injection (SQLi) is a code injection technique that allows attackers to interfere with the queries an application makes to its database. - In this lab, I explored SQLi vulnerabilities at different security levels (Low, Medium, and High) using DVWA.

Low Security Level

Description: At the low security level, user inputs are not sanitized, making the application highly vulnerable. –

Exploit: I entered `' OR 1=1--` to bypass the login.

Screenshot:

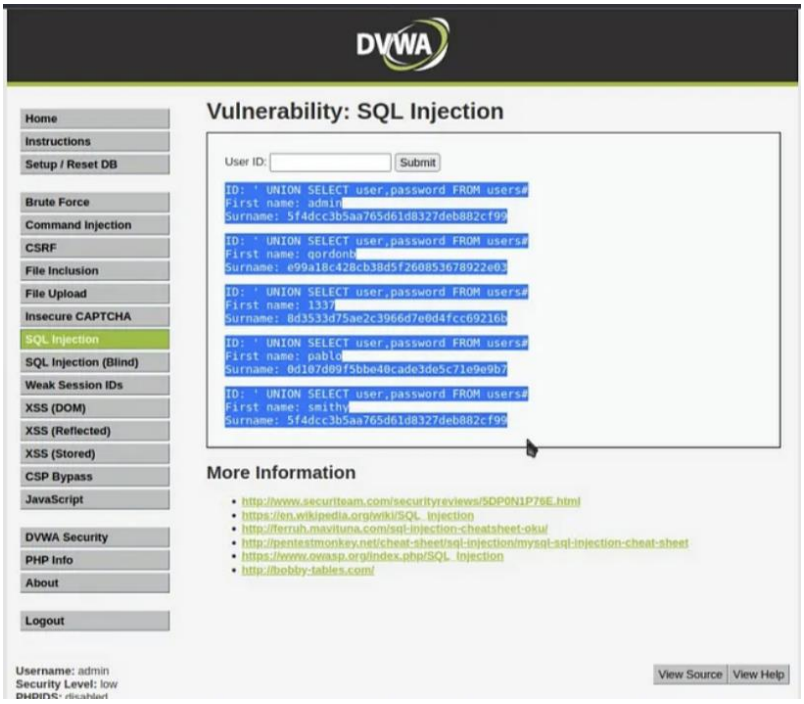
Outcome: Successful exploitation with data extraction.

Medium Security Level

Description: Medium security adds some basic input sanitization.

Exploit: Modified SQL injection payload to ' UNION SELECT column1, column2 FROM table_name#

Screenshot:



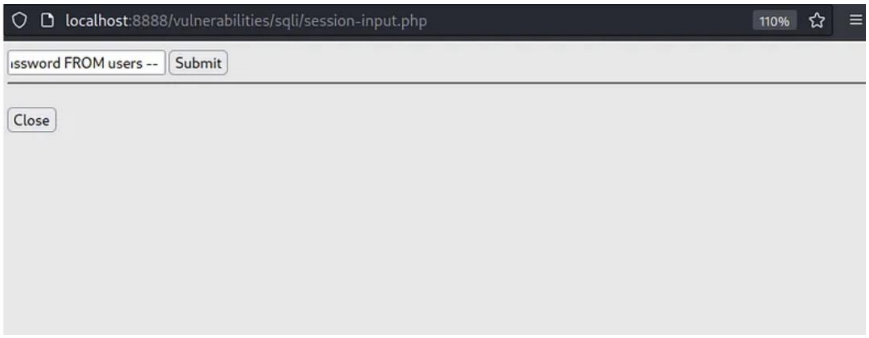
Outcome: Bypassed basic sanitization and retrieved data.

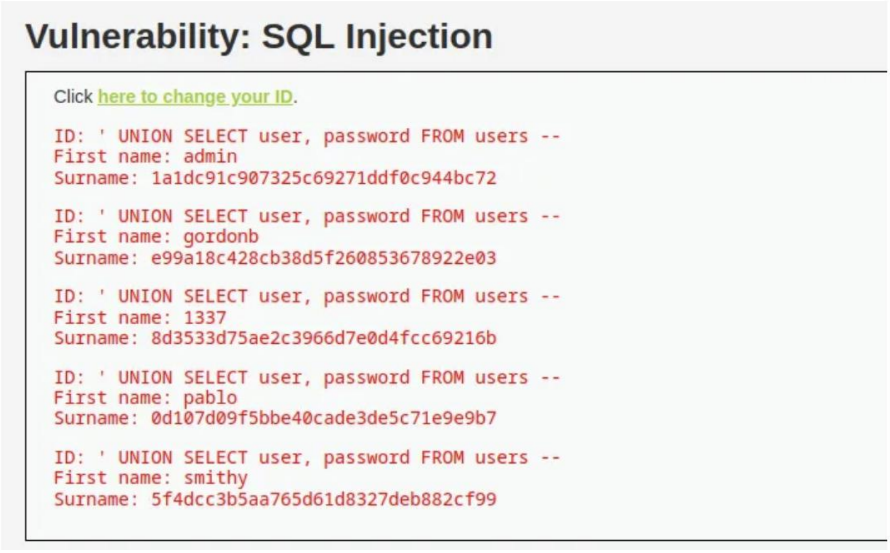
High Security Level

Description: High security implements strong input filtering and sanitization.

Exploit: ' UNION SELECT user, password FROM users --

Screenshots:





Outcome: Successfully bypassed advanced protections using the exploit