Lab 02: SQL Injection Login Bypass via Username Parameter

Lab URL (solved instance):

SQL injection vulnerability allowing login bypass:

https://portswigger.net/web-security/sql-injection/lab-login-bypass

Objective

This lab demonstrates how a vulnerable login mechanism can be bypassed using basic SQL injection.

The goal is to log in as the administrator user without knowing their password.

How the Application Works

When a user submits their credentials, the backend performs a SQL query like:

```
SELECT * FROM users WHERE username = '<input>' AND password = '<input>'
```

By injecting a payload into the username field and commenting out the rest of the query, we can bypass authentication logic.

Injection Payload Used

```
username=administrator'--&password=abc
```

'-- ends the SQL statement and comments out the password check.

This forces the query to become:

```
SELECT * FROM users WHERE username = 'administrator'--' AND password = 'abc'
```

Exploitation Steps with Screenshots

Step 1: Accessed the lab page (1-access-lab.png)

Step 2: Navigated to the login page (2-login-page.png)

Step 3: Intercepted the login request in Burp Suite (3-intercepted-login-request.png)

Step 4: Modified the request to inject payload and added CSRF token (4-modified-login-request.png)

Step 5: Successfully logged in and updated email to trigger solution (5-lab-solved.png)

Notes

- CSRF token was required to pass the login validation.
- Lab only marked as solved after performing an action as administrator (e.g. updating email).
- This shows that bypassing authentication alone isnt enough interaction as the admin is required to validate the exploit.

Repository Structure

Cybersecurity-Portfolio/

SQL-Injection/

Lab-2_SQL-injection-vulnerability-allowing-login/

1-access-lab.png

2-login-page.png

3-intercepted-login-request.png

4-modified-login-request.png

5-lab-solved.png