LAB06

Name: Truong Dang Truc Lam Students ID: B2111933 Class: M04 Date:17/09/2024

**System environment setting for pen-test**

| Resources | Sender(attacker) | Receiver(victim) | Homepage |
| --- | --- | --- | --- |
| OS | Windows |  |  |
| IP address |  |  |  |
| URL |  | http://localhost/Injection |  |
| Web browser | Chrome |  |  |
| CSS language |  |  |  |
| Web server |  |  |  |
| Web application |  |  |  |
| DB server script |  |  |  |
| Others |  |  |  |

Choose one exercise type and exercise

[Exercise type A]

Survey web security pen-test process model and explain it with the figure necessary

## **SQL Injection Example: A Login Page Vulnerability**

**Scenario:** A simple login page where users enter their username and password. The application constructs a SQL query to check if the credentials are valid.

**Vulnerable Code:**  
SELECT \* FROM users WHERE username = '$username' AND password = '$password';

**Attack:** An attacker might input the following username: admin'; --

The resulting query would become:  
SELECT \* FROM users WHERE username = 'admin'; --' AND password = '$password';

The -- comment symbol tells the SQL engine to ignore everything after it. This effectively bypasses the password check, allowing the attacker to log in as the administrator.

**Impact:** This type of SQL injection could lead to:

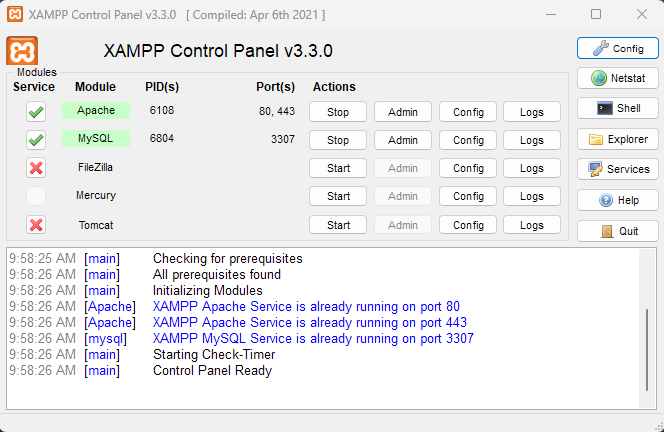
* **Unauthorized access:** The attacker could gain access to sensitive data or perform actions they are not authorized to do.
* **Data theft:** The attacker could steal personal information, financial data, or other valuable data.
* **Data modification:** The attacker could modify or delete data, causing significant damage to the system.
* **Denial of service:** The attacker could launch a denial of service attack by flooding the database with malicious queries.

**Prevention:** To prevent SQL injection, always use parameterized queries or prepared statements. These techniques separate the SQL code from the data, preventing attackers from injecting malicious code.

-GEMINI-

[Exercise type B]

XAMPP is a free and open-source software package that includes Apache HTTP Server, MySQL database, PHP programming language, Perl, and other components. It's a popular choice for developers and webmasters who want to create and test websites locally on their own computers.



Install XAMPP

1. Install web server (if necessary) => screen shot and explain in detail

Apache is a popular web server software that is used to serve web pages to visitors. It is free and open-source, and it is one of the most widely used web servers on the internet.



Install XAMPP

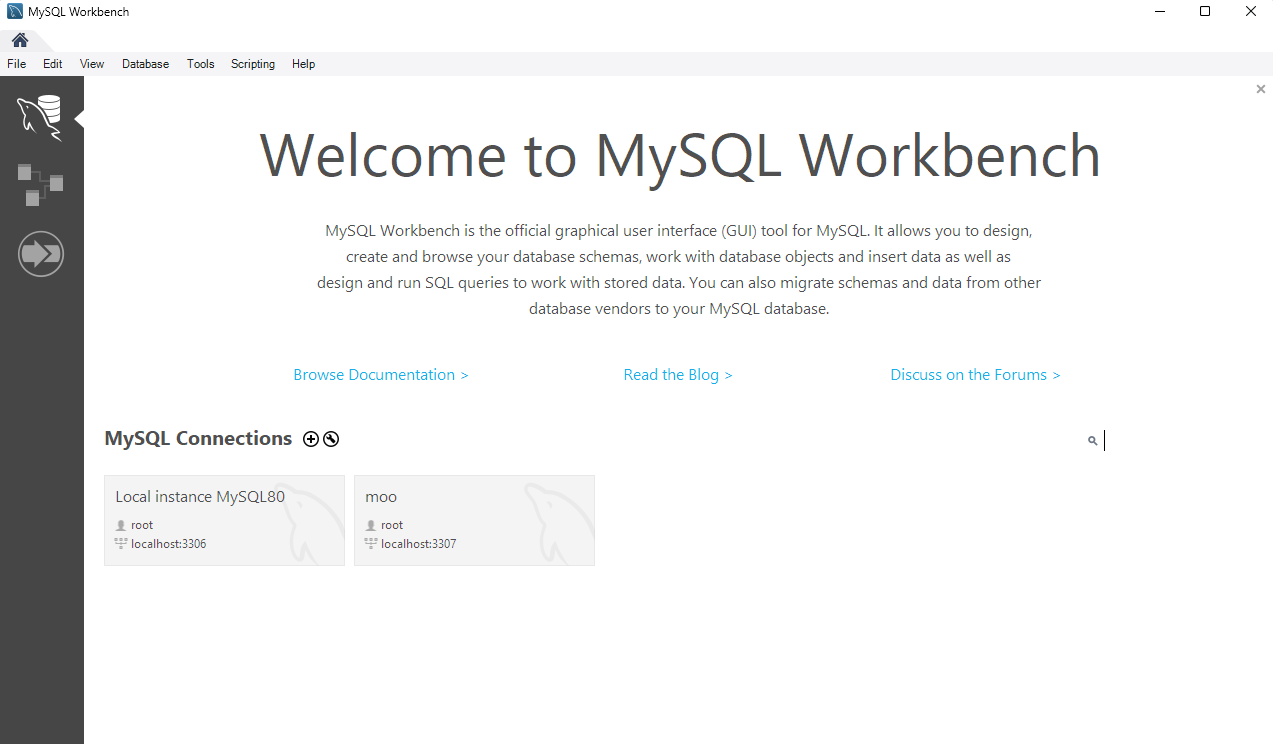
1. Install web application => screen shot and explain in detail





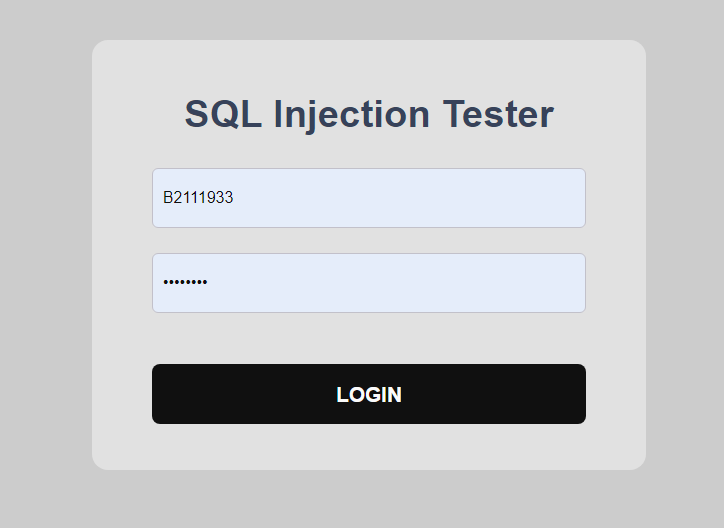
Code of my Web App

1. Install SQL DB server => screen shot and explain in detail



MySQL WorkBench

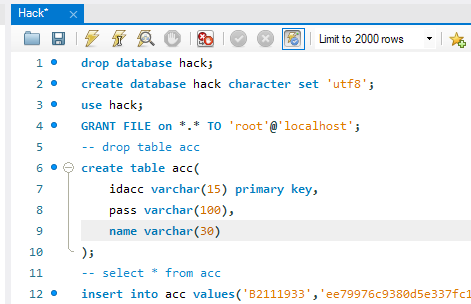
1. Develop client log in screen (if necessary) => screen shot and explain in detail



Client login screen

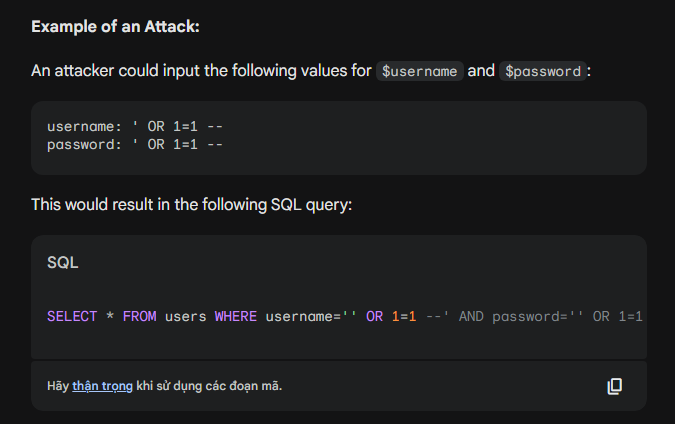
[Exercise type C]

1. Create SQL DB table(sharing with group table or not?) => screen shot and explain in detail



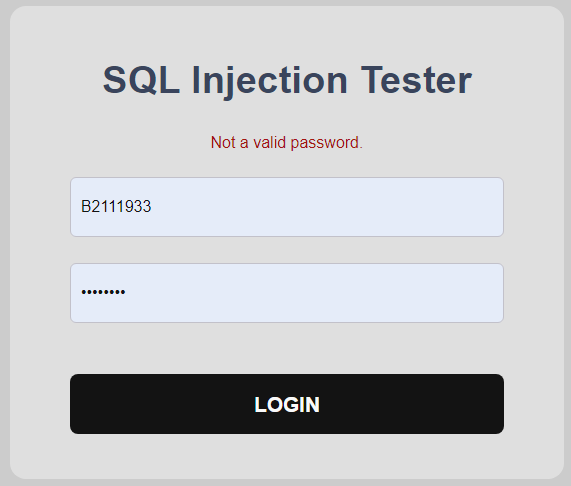
MySQL WorkBench

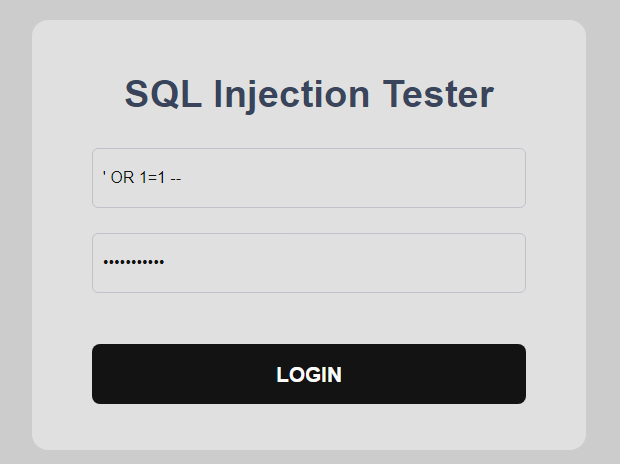
1. Create test data(ID,PW data,sharing with group table or not?) => screen shot and explain in detail

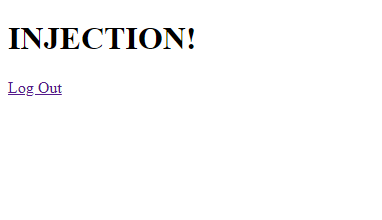


Injection code

1. **Connection test from client to** web application







SQL Injection