Lab - SQL Injection

SQL injection

SQL injection is one of the most common vulnerability in web applications today. It is one of the web hacking techniques that are very popular and dangerous because successful SQL injection could allow hackers to compromise your servers, networks, personal computers and confidential data. According to The Open Web Application Security Project Report released in 2017, SQL Injection is amongst the number 1 risks out of top 10 security risks.

What is SQL Injection? SQL injection is an attack injection technique that exploits vulnerability in SQL query via user's input data from client to the database layer of an application. This vulnerability exists in custom Web application that lacks proper input validation, fails to use parameterized SQL statements, and/or creates dynamic SQL with user-supplied data. It is occurred when user input is incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed.

Normally, attacker will test SQL injection by typing malformed SQL commands into front-end Web application input boxes that are tied to database accounts in order to trick the database into offering more access to information than the developer intended. A successful SQL injection exploit can read sensitive data from the database, modify database data, execute administration operations on the database, and recover the content of a given file present on the database file system and in some cases issue commands to the operating system. This attack allows attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, destroy the data and become administrators of the database server.

Task: SQL Injection

You need to use the browser and open localhost to perform this lab.

Login bypass is without a doubt one of the most popular SQL injection techniques. This lab will give explanations and a little deep understanding with some new flavors of bypasses.

Note: Please work through the information in the following link to understand how SQL query works: https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/

Your aim is to perform the following tasks.

I. Login when the Username is '123456789' but the Password is not known.

II. Login when both the Username and Password are not known.

III. Find table details containing all the Usernames and Passwords through SQL injection.

IV. Login into a specific user account by extracting the username and password from the table.

Based on your Observations from the above task, suggest possible defense in your lab submission document.