ITI3690 Intrusion Detection/Crisis Management

Project Title: Understanding and Mitigating SQL Injection Attacks

Completed By: Luswepo Daniel Sinyinza

Introduction:
In this project, I successfully completed a lab on SQL Injection (SQLi) attacks, specifically focusing on password bypass attacks. SQL Injection is a type of cyberattack where an attacker manipulates a web application's input fields to execute unauthorized SQL commands. This project aimed to provide a comprehensive understanding of SQLi, its mechanisms, and methods to prevent it.

Objective:
The primary objective of this project was to learn how SQL Injection attacks work and how to mitigate them effectively. I successfully achieved the following outcomes:

1. Performed an SQL Injection password bypass attack.
2. Analyzed why SQLi occurs and how to mitigate against it.

Key Terms:

- **SQL Injection (SQLi):** SQL Injection is a cyberattack method where an attacker executes arbitrary SQL commands on a vulnerable web application's database.

What I Learned:

1. What Is SQL Injection?
SQL Injection is a technique where attackers insert unauthorized SQL commands into a web application's input fields to manipulate its database. SQLi can be used to steal sensitive information such as passwords and credit card numbers.

2. Steps of a SQL Injection Attack:
SQL Injection attacks exploit security vulnerabilities in web applications by sending specially crafted requests to trick the application into running unintended SQL commands on the database. These commands can include inserting, deleting, modifying, or revealing sensitive data.

3. Execution of SQLi Attack in the Lab:
In the lab, I successfully executed an SQLi attack using a specific query. This query allowed me to bypass authentication and gain unauthorized access.

4. Preventing SQL Injection Attacks:

To prevent SQL Injection attacks, developers should validate user input from HTML forms and use parameterized database queries with bound, typed parameters. Server-side checking is also crucial to prevent SQL Injection.

Conclusion:

This project provided valuable insights into SQL Injection attacks and their mitigation. Cybersecurity, especially application security, plays a crucial role in safeguarding organizations against vulnerabilities and data breaches.

Additional Information:

- The project was funded by the Boston Area Advanced Technological Education Connections (BATEC) Grant No. NSF-0703097 through Bunker Hill Community College.
- The lab was conducted in a controlled virtual environment, ensuring the safety of real-world systems.
- Various challenges and discussion questions throughout the lab helped reinforce the learning experience.

Next Steps:

This project focused on the basics of SQL Injection attacks and their mitigation. For a deeper understanding and practical application, I plan to continue exploring related topics and conducting further penetration testing in the future.