John Munguia

CS 405 – Secure Coding

Module Two – SQL Injection Activity

July 13, 2025

Summary

In this activity, I implemented defensive coding practices to detect and block a specific type of SQL injection attack, specifically the "OR value=value" pattern. The goal was to ensure that when a user-supplied input attempts to bypass authentication logic or extract unauthorized data, the system would recognize the injection and stop the query.

To achieve this, I modified the run\_query() function. I used a lowercase copy of the SQL statement to look for a WHERE clause containing both " OR " and "=" a common structure used in SQL injection attacks (e.g., '1'='1', 'hack'='hack', etc.). If this pattern is detected, the system logs the blocked query and shows an error message, preventing it from executing.

This approach allows safe, expected queries to pass while rejecting potentially malicious ones.

A screenshot of a computer

AI-generated content may be incorrect.

**Build and Run Program Instructions (Visual Studio 2022)**

1. Open the included solution file SQLInjectionDefense.sln in **Visual Studio**
2. **Build** and then **Rebuild Solution**
3. Run the application using **Ctrl + F5**