**Module Two – SQL Injection**

**Justin Hancock**

**CS-405 Secure Coding**

**09.12.2024**

In this project, I have implemented protections against SQL injection attacks, specifically focusing on the “OR value=value” type of attack. The key steps were anticipating, preventing, reacting, and protecting the system from these attacks. The first step involved detecting suspicious patterns in SQL queries. I wrote the program to analyze each query for the presence of an “OR” clause, which is commonly used in SQL injection attacks. This helped in identifying queries that could be harmful before they were executed. Once the suspicious pattern was detected, the next step was to prevent the query from executing. The program checks both sides of the condition to see if they are identical. If this pattern was found, the system blocked the query from being executed. The system reacts by logging detailed messages to the console. This provides feedback to the console about why the query was blocked. Finally, for the queries that passed the initial checks and did not exhibit any suspicious patterns, the system will safely execute them. This makes sure that legitimate queries continue to function as expected while protecting against malicious ones. Overall, by breaking these into four stages – anticipating, preventing, reacting, and protecting – I was able to create a system that proactively detects and blocks SQL injection attacks, while providing clear feedback about the reasons for blocking or allowing a query.

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated