# **CS 405 2-2 Activity: SQL Injection Coding**

# **Austin Donaubauer**

# **Southern New Hampshire University**

# **CS-405 Secure Coding**

# **Wasim Alim**

# **July 12th, 2025**

# **CS 405 2-2 Activity: SQL Injection Coding**

This weeks activity dealt with detecting SQL Injection for input strings. The main attack was stated to be using “OR”. So, I created a loop to find the position of “or” in the sql string. If found, then I set the position of that found “or” to a integer variable to hold. I used that position to create a substring to hold the info of the string. I then looped again but through a vector list of SQL commands that are acceptable for this assignment such as “id=”, “name=”, and “password=”. Within that loop I used the string compare function to check if the substring matched any of the listed commands. If not, then I could output that there was an SQL Injection Attack and prevent the execution. I believe this approach catches any of the “ or “ injection attacks presented in this assignment.

Screenshot of my output from the program:

A screenshot of a computer

AI-generated content may be incorrect.