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

**Jason Farrell**

**Southern New Hampshire University**

A screenshot of a computer

Description automatically generated

I first determined by a std::cout debug statement the contents of the sql string for each good and injected scenario. I took the code TODO to heart to look for something more generic to flag and identify a possible SQL injection attack. I settled on using the string.find( ) method looking for substrings of “ or “ which should never be in a single field select statement. While I don’t really like just looking for this, I would have preferred to refactor the application to send different parameters and use a prepared statement for the SQL in a different way. Since this way would handle more complex SQL statements that would be required for other SQL Injection attacks. \