**SQL Injection Attacks**

James Porter

Department of Computer Science, Southern New Hampshire University

CS 405 Secure Coding

Professor Wasim Alim

September 11, 2022

**SQL Injections**

**Text

Description automatically generated**

**Summery**

This assignment has been a very tricky one, but I am trying my best. From what I can see, the first two inquiries are correctly executed with no malicious injections, but the last four do have malicious injections. I am still working out how to handle this issue, but I know that I need to check the statements with = signs to see if each side is the same.

I really struggled with finding a way to read the sql string without being able to change it at all. I tried lots of different solutions including writing a new string, but nothing worked. Eventually I came across the idea to check each sql string for = signs and then comparing the two values on either side. It is a process that is not very simple, but it works.

When an SQL search is initiated, the sql string is passed to this function that reads it and checks if there are any ‘=’ signs in the string. If there are not, then the code processes the search as normal with no issues. On the other hand, if there is(are) equal signs found, then the string is looked over to see if there is a value=value statement. Finally, if something is detected, the console will print out an error message that says an SQL injection was detected and no data will be printed out. This printed error would not be very practical to use, but for the purposes of this assignment, it shows where an injection might occur, and (for me) is easier to see that my code is working right.