Riley Snowe

CS 499

Southern New Hampshire University

22 May 2022

Milestone Two

The first artifact comes from my CS 405 Secure Coding class regarding SQL injection. The assignment was from our second week in the class where we had to write code that prevented SQL injection.

This artifact was chosen as it is very good to understand in detail. My CS 405 class did not go as in-depth as I would have liked with the assignment. When looking at the artifact from what was initially created, there are some improvements that can be made. As stated in the code review, I believe that the variables can be renamed to be more specific in what they are for, as well as additional comments.

SQL injection is when a user inputs data with a SQL command in a field normally used for logging into a system. The most basic commands are true and false, which could be 1=1 or a=a. The current program designed does protect against these basic commands. SQL injection has many different commands that can be used to attempt to bypass what is currently written.

Initially I stated that there could be a broader detective ability for the program, but after reviewing the code and methods of SQL injection, the current code should be efficient and enough to secure a program. The only additions would be to include more security in the SQL database itself such as using prepared statements with parameterized queries, which I do not have for this assignment.

I have already gone and renamed the variable for detecting inputs that could be SQL injection, as well as adding more comments. I also reworded some existing comments to be more precise with the operations that are being preformed with the if statements. I believe the changes added further improve the readability of developers regarding their understanding of the code. The code protects against SQL injections as injections need to use an equal sign, which is looked for in both the number and word injection detections. Any other security related issues would be outside of this specific program when related to the application.

The next page shows pictures from the program before and after changes. The only changes made are the variable names and changes to comments.

Before Changes:

Text

Description automatically generated

After Changes:

Text

Description automatically generated