Daniel Coffey

2-2 Activity: SQL Injection Coding

CS 405 Secure Coding

01/30/21

For this assignment, I was tasked with fixing the run\_query method so that it would fail and display an error if there is a suspected SQL injection. I also couldn’t flag 1=1 as an error since 2=2 will work just as well. The process of this was straight forward. My first step was to declare my variables. The first variable I declared was tempString, and it was a temporary string, which was a text version of SQL. The second variable that I declared was newSQL, which was a sanitized SQL string. I then declared a smatch variable. Smatch is instantiation of the match\_results class template for matches on string objects. This variable was titled match. This would look for the pattern match within the strings. I then declared two regex variables. One variable was for number injection and the other was for word inject. The number injection had the purpose of finding the pattern to match for “OR 1 = 1;”, whereas the word injection had the purpose of finding the pattern to match for “OR “he” = “he”;”

The next step was to search for and detect the SQL injection pattern match. If it was detected, the margins would be replaced with a semicolon and the query would be rerun using the sanitized SQL string “newSQL”. I had this set up as two if statements, one for numeric and the other for alphabet matches.

