Southern New Hampshire University

CS 405 Secure Coding

Module 2 -- SQL Injections

George Harrison Jr

RESULTS:

Text

Description automatically generated

Text

Description automatically generated

In approaching the SQL injections assignment, first the code was familiarized with. I went through each function to understand the flow of the functions used in the main. It appears that the main function initializes the database as “db” and if the database connection is established the function run\_queries() is executed. This function is passed the database connection then performs an series of calls to the run\_query function and checks the functions executions. If run\_query successfully returns the data from the query is returned.

It was inside the run\_query function where changes were made to ensure that SQL injections could be prevented. The approach was to secure the “sql” variable containing the query by using a prepared statement. This will escape the text for all the parameter values provided. Protecting against SQL injections. Once prepared the statement was executed the bind\_parameter\_count() was used to lock into a statement and step was used to step through the statement. Once executed, the statement was the reset then finalized to close the statement. The idea here is to prevent injections by only allowing the prepared statement access to the query would be the only request sent to the database for the desired user data to be successfully returned.