**SQL Injection Coding**

Justin Starr

Department of STEM

CS 405 – Secure Coding

Professor Mike Alesso

July 14, 2024

**SQL Injection Coding**

**Screenshot**

**A screenshot of a computer

Description automatically generated**

**Process Summary**

The way I approached this problem was by first having an understanding of what the program needs to look for to know when a possible SQL injection attack is about to occur. We know that the specific type of SQL injection attack that is used in the program is the “OR value = value” attack. Therefore, we can determine whether or not a query contains a possible SQL injection attack by looking for the keyword “or” throughout the SQL query string. If the SQL string contains the keyword “or”, we then split each word in the string into separate tokens and store them in a vector data type. This allows us to inspect the query further by splitting the last token of the query into additional tokens using an equals sign as the new delimiter. These additional tokens are stored in a new vector data type that can be used for comparing the values of each token. If the two values extracted are equal to each other in any case, a possible SQL injection is detected. The program displays an error message to the user and the method is failed. This function will work in all cases in which the program attempts to use SQL injection because it will always first look for the keyword “or”, and then it will compare the two values in the last parameter of the SQL query to determine if value = value or not. If the two values are equal the suspected injection is prevented, thereby protecting the code from SQL injection attacks.

The main issue I encountered was figuring out how to separate the SQL query in a way that I would be able to make a value = value comparison. Fortunately, I just finished a course where we worked with various data structures, and I was able to use the knowledge gained from that course to help me use vector data types to solve this problem.