**Console application running SQLInjection.cpp**

Text

Description automatically generated

To detect potential SQL injections within this application, I started by creating a new function named *is\_valid\_query* which returns a Boolean if the SQL query is valid or not. The first thing it does is look through the SQL query to see if an or operator is present. If it isn’t, it can be assumed that a simple select \* query is present, and no SQL injection is present. If an or operator is present, then I set the starting value to the position of where the or operator is present plus 2 values for the values o and r. I then perform a substring to find values with an equality operator and split them into a string vector.

For each item present within the string vector, I take the first index value of the string vector and compare it with the rest of the entries present similar to how I perform the search for the or operator. If the first index value is in a string value in one of the remaining indices of the vector, it can be assumed that a potential SQL injection is present. In this scenario, false is returned to the calling function and the message “Potential SQL injection detected” is written to the console and the application continues with its next functions.