2-2 Activity: SQL Injection Coding

Joel Meza

Professor Trevor Hodde

January 13, 2022

CS 405 – Secure Coding

Southern New Hampshire University

**Overview**

When working on this assignment I encountered a series of ideas in which I can grab the SQL Injection from the code. Once I examined the code, I detected the injection once the brief code statement went on, there I instantly thought it through where I can separate the components and evaluate the string to figure what really is the potential SQL injection. Considering my first method was to separate the ‘or’ within the spaces that are practical which could only work on statements already used where a malicious user would position it its parameter ‘value’ if any spaces are available in between. Therefore, I had to emphasize on parameter ‘value’ where I know the parameter ‘value’ has single quotations marks around this can be taken in consideration to separate the parameter’s value for leveraging the situation out. As I look in depth with the single quotations of the given parameter’s value, I would be able to discern and predict the end of the given statement. For example, any value given after the second quotation could be at the risk for a possible SQL injection. Eventually, by determining that after the second quotation found that is the final character in the string, then it confirms to me that no other statement would be completed.

However, if a software engineer would like to apply some additional SQL statements into the code, then it’ll be required to secure and authenticate before doing so for any future possible malicious SQL injection. Although, this will consume more complexity to the program in which it could become further useful to modify and efficient. In terms of querying the cursor to proper given parameters in each part of the selected argument statement from the SQL dataset given. This method can help to our advantage which makes the program more reliable, secure, and gives the ability to analysis in depth against user input without even enhancing more complexity to SQL statements rather than trying to divide a whole query in portions later to obtain best results for future risks of Text

Description automatically generatedText

Description automatically generatedmalicious SQL statements.