**Module Two SQL Injection**

Joseph Veneski

Department of Computer Science, Southern New Hampshire University

CS-405 Secure Coding

Professor Kaan Esendemir

March 17, 2024

**Module Two SQL Injection**

**Summary:**

To help mitigate SQL Injection attacks in the provided code, a Prepared Statement was used. Instead of treating the input as part of the SQL Query itself, the input is treated as a value that replaces the ‘?’: 

This helps to safeguard the query from attempted alterations by defining the SQL code ahead of time and pass in parameters (The Coding Interview, 2017).

In addition to nullifying any attempted injection to this query, a heuristic search is implemented to detect common injection signs. If any of the listed symbols appears within the input, the user is notified:

A computer screen shot of a program code

Description automatically generated

These two measures suffice for the current model to detect and mitigate injection threats to the code base. If new queries are written or used, new prepared statements will need to be created to handle additional functionality.

A screenshot of a computer program

Description automatically generated

**References**

The Coding Interview. (2017). *IQ 27: How to Prevent SQL Injection* [Video]. YouTube. <https://www.youtube.com/watch?v=mo8RsfhtUG8>