Module Two SQL Injection

Jordan Whitney

CS-405 Secure Coding

Professor: Alan Spencer

7/11/2025

For the SQL injection protection implementation, I wanted to enhance the “run\_query()” function to detect and prevent SQL injection attacks in the form of “OR value = value”. These are attacks that are commonly used to bypass authentication by injecting tautologial expressions like “1=1” or “abc”=”abc”. I added logic inside “run\_query()” to scan the input SQL for any suspicious patterns. The code converts the SQL to lowercase for case-insensitive detection, it looks for “or” in the SQL statement and extracts the part of the query after “or” and normalizing that by removing the whitespace and semicolons. Then checks for numeric tautologies and string tautologies “hank”=”hank” using regular expressions. If a tautology is found it prints a warning message to the console, and prevents the query from executing by returning “false”. A screenshot of a computer

AI-generated content may be incorrect.