Joseph Les

CS 405 Professor Hodde

SQL Injection Coding

To enhance the security of an in-memory database against SQL injection attacks, a modification was made to the `run\_query` function in the provided C++ code. The primary goal was to detect and prevent the "OR value=value;" type of SQL injection and inform the user via console messages.

Key updates include the addition of necessary C++ standard library headers such as `<tuple>`, `<regex>`, and `<ctime>`. This ensured the code could utilize modern C++ features effectively. The core change involved implementing a regex pattern in the `run\_query` function to detect suspicious SQL injection patterns like "or 1=1" or "or 'a'='a'", both case insensitive.

When such patterns are detected, the function outputs "Potential SQL Injection detected. Query aborted." to the console and halts the query execution, preventing malicious commands from running.

Testing confirmed that the program successfully created and populated the `USERS` table, executed legitimate queries, and effectively detected and prevented SQL injection attempts. This modification significantly enhances database security by proactively identifying and blocking common injection patterns.

