Douglas Rowland

CS-405

SQL Injection Defense

Approach:  
The run\_query() function was updated to detect and prevent SQL injection attacks. It scans the SQL query for patterns like "OR value=value", including common variations (e.g., "OR 1=1;"). If a potential SQL injection is detected, the function logs an alert and prevents query execution. Legitimate queries are allowed to proceed as usual.

How it works:  
This solution prevents the specified attack pattern from executing. By checking for key indicators of injection and blocking suspicious queries, the program mitigates the risk of unauthorized data access.

Issues and Resolutions:

* Issue: Case-sensitive detection could miss malicious patterns like Or or oR.  
  Resolution: The query string is converted to lowercase for consistent detection.
* Issue: Overly strict checks could block legitimate queries.  
  Resolution: The detection logic was refined to focus only on injection-like patterns (OR combined with an equality check).

Basically, SQL injection is someone trying to sneak in commands to get access to the sensitive data (or database in this case). I updated the code to spot these sneaky commands; specifically, the kind where someone tries to trick the system using "OR value=value." If the program detects this kind of behavior, it blocks the action and logs a warning. This allows only safe and intended queries are run, protecting the database from unauthorized access.

A screenshot of a computer

Description automatically generatedScreenshot of Console Output: