CS405

Merrik Wright

Module 2

Approach Taken:  
 To complete the assignment, I modified the run\_query() function to detect and block malicious patterns such as OR value=value. I used a C++ regular expression to identify cases where user input contained SQL literals that could bypass authentication logic. The regex pattern matches classic injection forms like OR 1=1, OR 'x'='x', etc, like the assignment sai.

How It Works:  
 Before executing the SQL query, the program scans for any injection pattern using std::regex\_search(). If a match is found, the query is not executed and a message is printed to the console. This prevents the database from returning unauthorized data.

Issues Encountered:  
 Initially, Visual Studio showed a linker error due to having two main() functions. I resolved this by removing the auto-generated SQLInjectionProject.cpp. Once cleaned up, the solution compiled and ran correctly. I forget that it created the default .cpp file every time.

Results:  
 The console output confirms that legitimate queries work, while all injection attempts are blocked as expected. The solution successfully mitigates this class of SQL injection vulnerability. I believe the screenshots are what were requested, but I can take new ones if needed.

