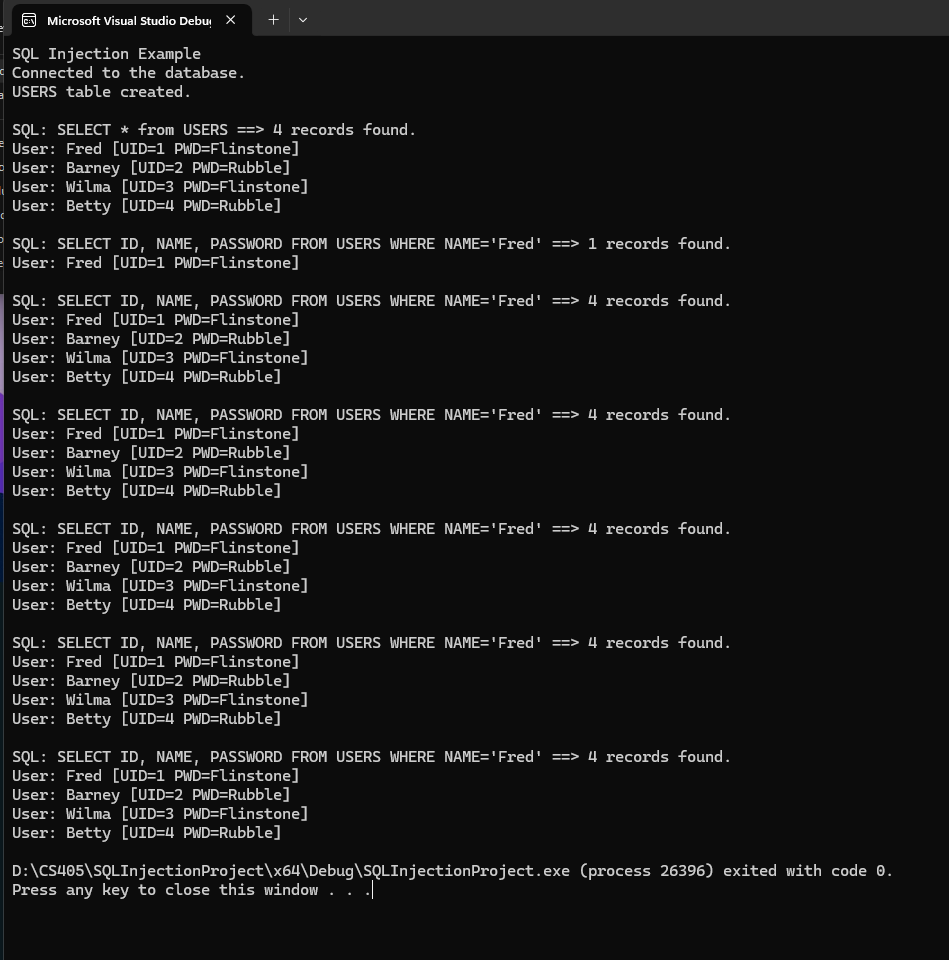
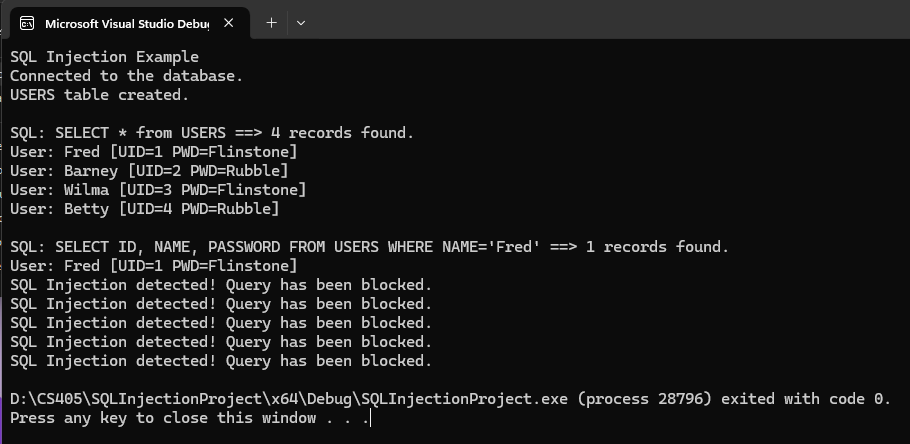
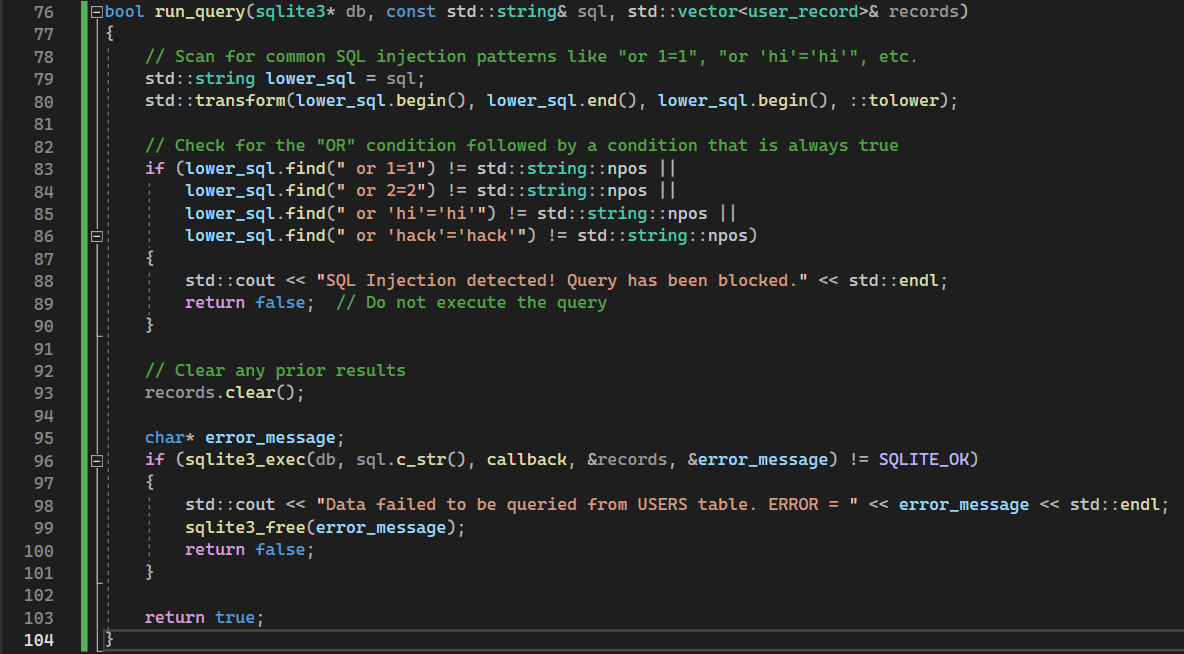
**Original SQL Output**

**Updated SQL Output**

**Changed run\_query code**

**Summary**

In this assignment, I implemented safeguards within the run\_query() function to detect and prevent SQL injection attacks. Specifically, I added logic that scans for common SQL injection patterns such as "or 1=1", "or 2=2", and similar conditions that always evaluate to true. By converting the entire SQL query to lowercase, I ensured the checks are case-insensitive, allowing the program to detect these patterns regardless of how they are written. When such an injection pattern is detected, the program blocks the query and logs a message stating that the SQL injection was detected. These changes prevent malicious users from executing unauthorized queries and ensure that only legitimate SQL commands are run against the database. Additionally, I retained the original functionality, where, if no injection is found, the query proceeds as normal. This modification effectively closes the security loophole that was exploited by SQL injection.