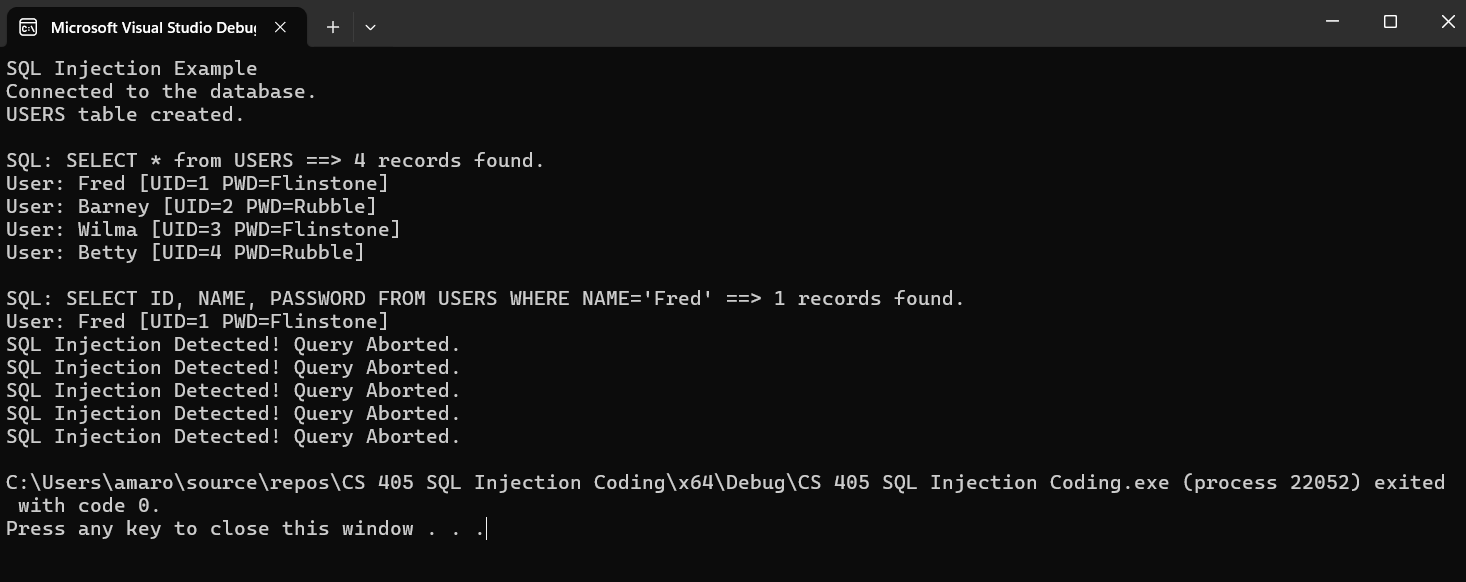
2-2 Activity: SQL Injection Coding

**Screenshot**

****

**Summary**

In the SQL Injection Coding activity, we were presented with code that attempts SQL injection in the form of “OR value=value” attacks. We were tasked with anticipating, defending, and communicating potential SQL Injection attacks. To accomplish these tasks, modifications were necessary within the run\_query() function. I utilized an if statement that checks if SQL queries contain the characters “ or “ and “=” through sql.find(“ or “) and sql.find(“=”).

This approach ensured that any tested “OR value=value” attack was properly detected and prevented, as many of the tests within the program tested different values such as 1=1, 2=2, and so on. Next, if the if statement caught a query containing the characters “ or “ and “=”, a simple print statement is used to inform the user that an SQL injection is detected and that the query is aborted. This is then followed by a return false to prevent the SQL injection attack.