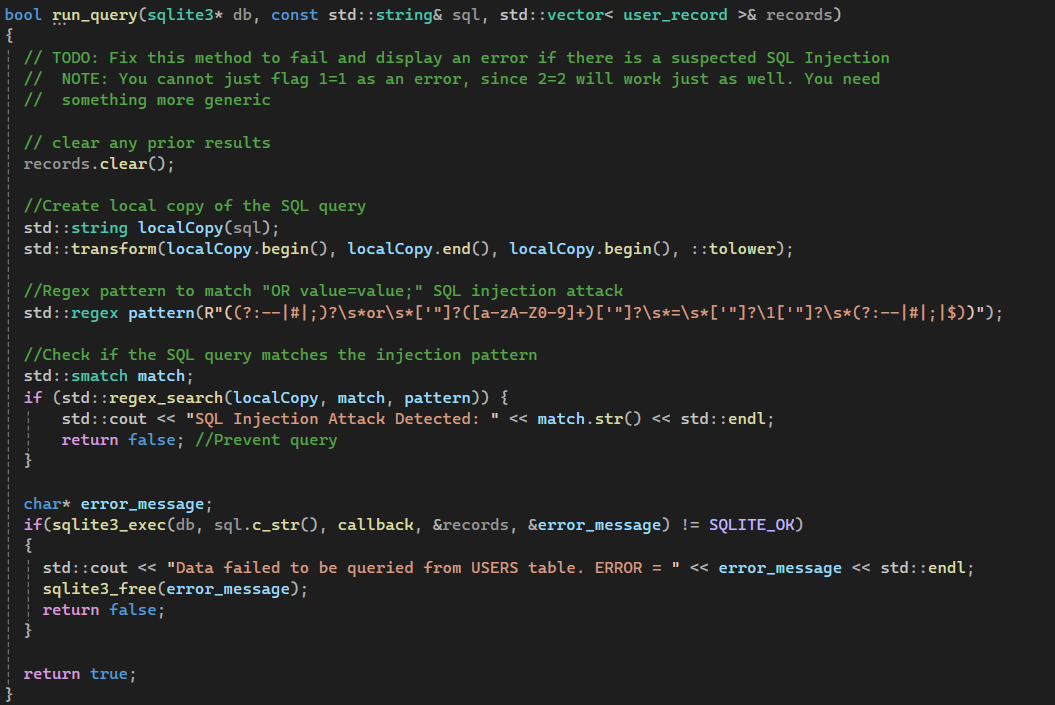
CS 405

SQL Injection

Caleb Ewer

1/04/2024

Code Snippet:



Output before change:

A screenshot of a computer

Description automatically generated

Output After Changes:

A screenshot of a computer

Description automatically generated

Explanation:

I began by creating a local copy of the SQL query string to ensure the original query remains unaltered. This local copy was converted to lowercase to simplify regex matching and make the detection case insensitive.

Next, I created a regex pattern to detect potential SQL injection attempts. The pattern specifically checks for:

* SQL comments (--, #) or a semicolon (;) appearing before the OR keyword.
* The OR keyword itself, allowing for spaces before or after.
* A literal value consisting of letters, digits, or both, optionally enclosed in single or double quotes.
* The = operator, allowing for spaces before or after.
* A tautological condition where the second value matches the first captured group (e.g., OR value=value).
* SQL comments, a semicolon, or the end of the string, ensuring proper query termination.

I then added a check to see if the local copy of the query matched the regex pattern. If a match was found, a message was displayed indicating that an SQL injection was detected, along with the problematic portion of the query. This prevented the query from being executed, thereby blocking the injection attempt.