Tonya Sanders

CS 405

Mimi Tam

09/15/2024

A computer screen shot of a black screen

Description automatically generated

To effectively detect potential SQL injection attempts, it was necessary to include the regex library, as it provides a robust mechanism for pattern matching. SQL injection attacks often exploit logical operators like "AND" or "OR" combined with improper input to manipulate the query. The challenge was to identify these operators in a generic way without relying on specific cases like "1=1" or "2=2." The use of regular expressions allowed for a more flexible and generalized approach, scanning for logical operators followed by improper or missing delimiters. By integrating regex with case insensitivity (icase), the code could detect suspicious patterns regardless of capitalization or minor variations in the attack syntax. Once a match is found, the code flags the query as potentially malicious, preventing it from executing.