Larry Arndt

CS-405

January 14, 2023

SQL Injection

With SQL injection hackers are trying to modify and append a true condition on to the end of a query. They do this to infiltrate and break through the database defense and get all the usernames and passwords in the database. For my defense I queried the SQL statements for the word or, which is used in these attacks. If the SQL statement comes in with the word or in it may be an attack, and you need to take additional steps to protect against the incoming statement.

The way I am doing this in this exercise is trapping the statement as a single statement to go in to the database to be checked by itself. The flag is if the stamen has the characters or in it, which prompts a possible SQL injection, but could also be part of a username. Also just wrapping all username entries could be a valid idea and probably smart idea. Prepared statements and stored procedures are also smart ways to go where you parameterize your inputs.

The method I have created here strips the ‘ characters from the entire statement and then inserts one single quote at the start of the username and one at the end, so the whole entry is processed as the username entry. If a user is legit this will do nothing to their input, but if it is an injection attempt it will cause it to fail because there will be no match to that username string and it prevents the attack, because the or something is equal to something piece is deactivated.

Text

Description automatically generated