In the original code it was possible for a hacker to hack into the database using SQL injections. This needs to be blocked/prevented in order to keep the data secured for the company. What needs to be done is adding a library to detect patterns and prevent from being hacked. Below is the code before editing.

Text

Description automatically generated

I added in the regex library, which is short for regular expressions. This library “…is a sequence of characters, used to search and locate specific sequences of characters that match a pattern” (Barnhill, 2021). It uses metacharacters to help define a pattern and also comparators like “LIKE” and “SIMILAR TO” to find matching strings. Using the regex library, I am able to help the company detect any SQL injections. If someone were to try to hack using SQL injection, I have edited the code to send a warning message that someone is trying to hack into the system. Said error message will then block the hacker from getting into the database. See image below to updated code where there was a detection of SQL injection, warned the user, and blocked access.

A screenshot of a computer screen

Description automatically generated with medium confidence

References

Barnhill, B. (2021, August 9). *How Regex in SQL Works*. The Data School. Retrieved May 13, 2022, from <https://dataschool.com/how-to-teach-people-sql/how-regex-works-in-sql/>