SIT 218/738: Secure coding

**Pass task 5.2C: SQL injection**

**Overview**

In the SQLInjection webapp is vulnerable to SQL injection. Use the username ‘Alice’ to inject a crafted input to login to the application without the password. The vulnerable code file is located in

A screenshot of a computer

Description automatically generated with medium confidence

Highlight the vulnerable code in the functions **existsClient** and **areCredentialsCorrect**.

Write the safe SQL query code with PreparedStatement.

**Submission Requirements:**

Submit one PDF file containing the following information:

1. Screenshot of the bypassing the authentication without the entering the password.
2. Screen shot or piece of vulnerable code and why is it vulnerable.
3. The correct piece of code. (you don’t have to execute and show the output)

**Submission Due**

The due for each task has been stated via its OnTrack task information dashboard.