String SQL Injection

Saturday, November 4, 2017 11:46 PM

SELECT * FROM user_data WHERE last_name = 'user input'

- The website automatically adds a ' at the end of your input
  - Escape it by adding a comment at the end of your statement
  - Enter in the input field..

  ' OR 1=1 --

String query = "SELECT * FROM employee WHERE userid = " + subjectUserId;