<table>
<tr><td>  </td><td colspan="3">King Saud University
College of Computer and Information Sciences
Department of Software Engineering</td></tr>
<tr><td rowspan="6"></td><td colspan="3"></td></tr>
<tr><td>Course Code:</td><td colspan="2">SWE 314</td></tr>
<tr><td>Course Title:</td><td colspan="2">Software Security Engineering</td></tr>
<tr><td>Semester:</td><td colspan="2">Fall 2019</td></tr>
<tr><td>Assessment</td><td colspan="2">Course Project</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td rowspan="6">Students</td><td>Name</td><td>ID</td><td rowspan="2">Total Points

10</td></tr>
<tr><td>Ahmad Alsudairy</td><td>438102086</td></tr>
<tr><td>Abdulaziz Almuaither</td><td>438102736</td><td rowspan="4">Deadline Date
November 30nd</td></tr>
<tr><td>Mohammad Alqahtani</td><td>438160466</td></tr>
<tr><td>Omar Basaqer</td><td>438102442</td></tr>
<tr><td>Abdullah Alshalan</td><td>438103354</td></tr>
<tr><td>Section No. / Day Time</td><td colspan="2">73556 / Monday 1-2 PM</td></tr>
</table>

Project Description

The following code represents a banking function that takes the account number and password from the user and displays the account information using an SQL query.

You are required to secure the program from SQL injections using **three** different techniques.

You should submit the .java file through LMS along with this document with your names on it.

```java
import java.util.Scanner;
public class Banking {

    public static void success(){
        System.out.println("Success!");
    }

    public static void failure(){
        System.out.println("Invalid Input");
    }

    public static void main(String[] args) {
        Scanner scanner = new Scanner(System.in);

        System.out.println("Enter Your Customer ID");
        String customerId = scanner.nextLine();

        System.out.println("Enter Your Password");
        String customerPwd = scanner.nextLine();

        String sql = "select "
                    + "customer_id,acc_number,branch_id,balance "
                    + "from Accounts where customer_id = '"
                    + customerId
                    + " and customer_pwd = '"
                    + customerPwd
                    + "'";
        // Connection c = dataSource.getConnection();
        // ResultSet rs = c.createStatement().executeQuery(sql);
        success();
    }

}
```

***Note:** The SQL Connection statement is commented out so you can run the system.

We are secure the program from SQL injections using these different techniques:

1. **Input validation.**

2. **Enforce least privilege (hide id, pwd from user):** Make sure connections to the DB use the least privilege necessary.

3. **Watch out for canonicalization:** input should be decoded before trying to sanitize it.

4. **Avoid simple escaping:** Simple escaping (for example, string replace functions) are weak and have been successfully exploited.

5. **Avoid detailed error messages:** The attacker can use the information generated in the error message to construct an attack.