**Security discussion:**

In this case we can find a common security vulnerability that can lead to a SQL Injection attack.

A SQL Injection attack is an attempt to run an unauthorised code on the SQL server side, this is a code injection technique that might try to destroy your database or access unauthorised information. This usually happens when dynamic database queries are created that include user input.

In the example provided the problem with the code is that we’ve put the customer\_id’s value into a query with no validation. If the variable is populated with a web form or open input, there are different ways that the database can be accessed and abused.

One of the most popular tactics to avoid this would be: Parameterised Queries. This technique consists in the use of prepared statements with variable binding or placeholders in our queries whenever we need to insert a value given by the user. They are simple to write and easier to understand. Parameterised queries are the most common tactic to make sure any hacker is able to change the query created by the developer, even if a SQL command is injected.