The security implications of the code supplied is a very common attack called SQL injection. This works because the customer Id’s value doesn’t have any form of validation. Using tools like Insomnia and postman a hacker can change user requests sending SQL code as data therefore bypassing any client-side validation. This will allow them to send SQL code for example they could post in the following code “2 or 1= 1” this will change the executed SQL code to “SELECT \* FROM table WHERE customer\_id=2 or 1=1”. “1=1” will equal true and will return all the data from the table. This method of injecting code opens up the application to many attacks like Union based SQL injection to obtain data from other tables. Time based SQL injection which passes the code execution for an amount of time slowing down the server.

To prevent these types of attacks Prepared Statements can be used when executing the query. These prepared statement are commonly known as getter and setters where it treats these values from requests as data, this would prevent the change of intent of the query and would therefore look for a customer id that would equal the string “customer\_id=2 or 1=1” rather than executing the query as SQL code.