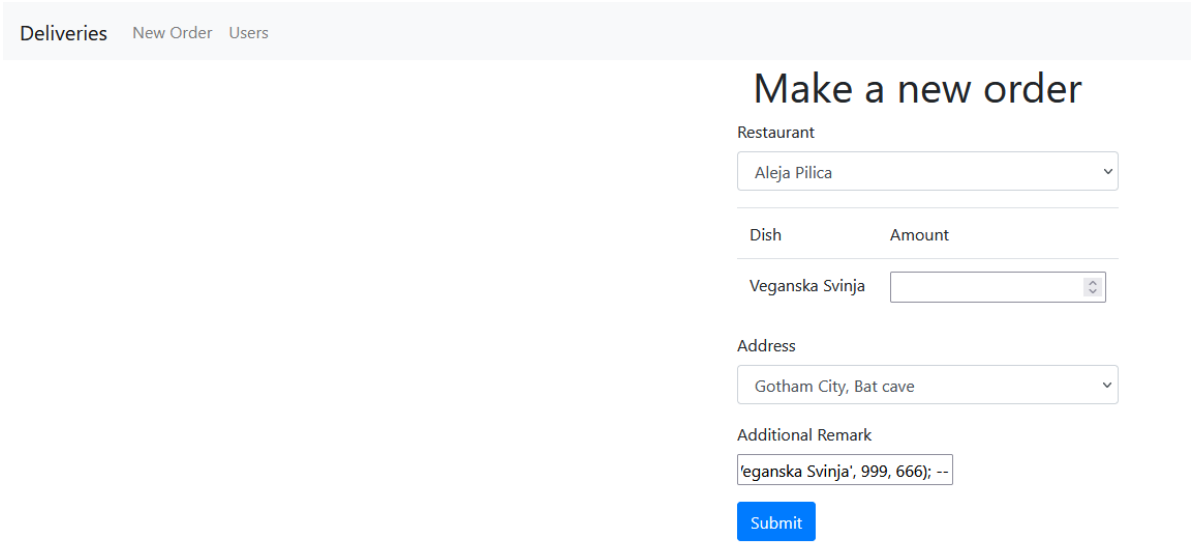
SQLi Izvestaj

U ovom zadatku je iskoriscen SQLi napad pomocu instrukcije:

```
'); INSERT INTO restaurant (id, name, address, typeid) VALUES (666, 'Aleja
Pilica', 'Kokos I Mokos 22', 2); INSERT INTO food(id, name, price, restaurantId)
VALUES (666, 'Veganska Svinja', 999, 666); --
```



Kao sto se vidi na slici, "Aleja Pilica" je dodat kao opcija za biranje.

Zastita

U resenju je uocena slabost da se konkateniraju Stringovi bez ikakve provere.

```
public void insertNewOrder(NewOrder newOrder, int userId) {
    LocalDate date = LocalDate.now();
    String sqlQuery = "INSERT INTO delivery (isDone, userId, restaurantId,
addressId, date, comment)" +
            "values (FALSE, " + userId + ", " + newOrder.getRestaurantId() + ",
" + newOrder.getAddress() + "," +
            "'" + date.getYear() + "-" + date.getMonthValue() + "-" +
date.getDayOfMonth() + "', '" + newOrder.getComment() + "')";
    try {
        Connection connection = dataSource.getConnection();
        Statement statement = connection.createStatement();
        statement.executeUpdate(sqlQuery);
```

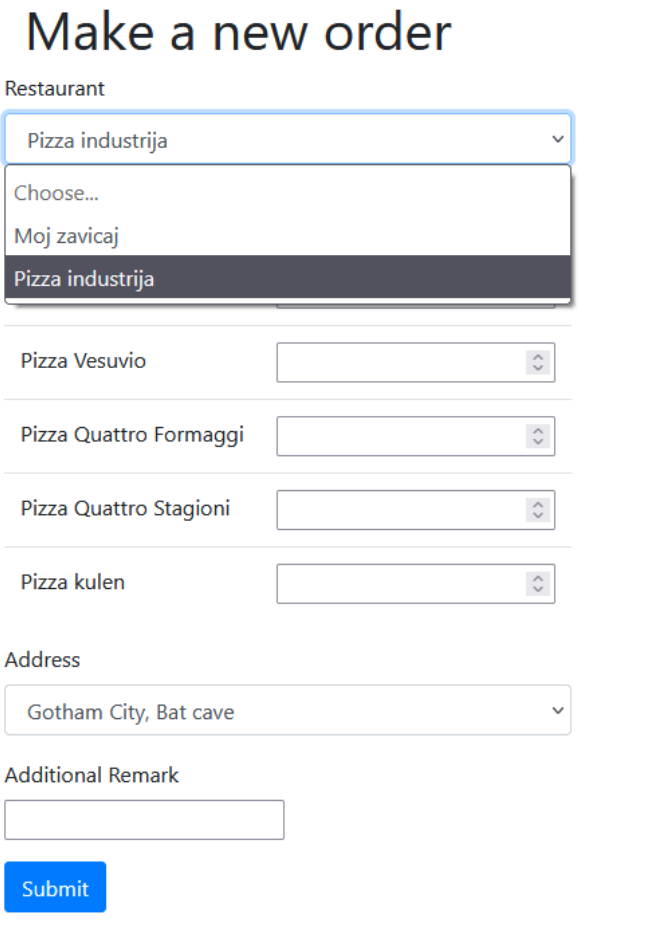
Kako bismo resili ovo, a ujedno sto manje koda izmenili, neophodno je koristiti `preparedStatement` umesto `createStatement`

Kada izmenimo, dobijamo sledeci kod:

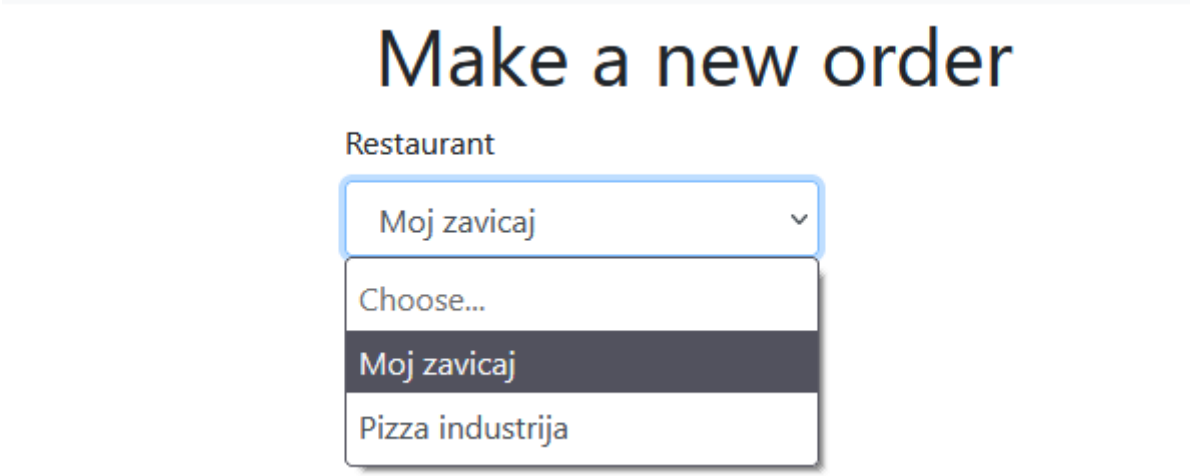
```
public void insertNewOrder(NewOrder newOrder, int userId) {
        LocalDate date = LocalDate.now();
        String sqlQuery = "INSERT INTO delivery (isDone, userId, restaurantId,
addressId, date, comment) VALUES (FALSE, ?, ?, ?, ?, ?)";
        try (Connection connection = dataSource.getConnection();
             PreparedStatement statement =
connection.prepareStatement(sqlQuery)) {
            statement.setInt(1, userId);
            statement.setInt(2, newOrder.getRestaurantId());
            statement.setInt(3, newOrder.getAddress());
            statement.setString(4, date.getYear() + "-" + date.getMonthValue() +
"-" + date.getDayOfMonth());
            statement.setString(5, newOrder.getComment());
            statement.executeUpdate();
```

Ako bismo istestirali ovaj kod, trebalo bi da sve ostane nepromenjeno:

PRE



POSLE



Ali:

Delivery

ID	8
Status	Not deliverred
Date	2022-01-15
To user	bruce
From restaurant	Pizza industrija
To address	Gotham City, Bat cave
Comment	'); INSERT INTO restaurant (id, name, address, typeid) VALUES (666, 'Aleja Pilica', 'Kokos I Mokos 22', 2); INSERT INTO food(id, name, price, restaurantId) VALUES (666, 'Veganska Svinja', 999, 666); --

Vidimo da je naredba "obradjena" i upisana u tabelu!