

# 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); --
```

Deliveries New Order Users

## Make a new order

Restaurant

Aleja Pilica

Dish

Amount

Veganska Svinja

Address

Gotham City, Bat cave

Additional Remark

'eganska Svinja', 999, 666); --

Submit

## Zastita

U resenju je uocena slabost da se konkatenuiraju 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, " + userId + ", " + newOrder.getRestaurantId() + ",
" + newOrder.getAddress() + ", " +
        "'" + date.getYear() + "-" + date.getMonthValue() + "-" +
date.getDayOfMonth() + "', '" + newOrder.getComment() + "');"
    try {
        Connection connection = dataSource.getConnection();
        Statement statement = connection.prepareStatement(sqlQuery);
        statement.executeUpdate(sqlQuery);
    }
}

```

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

## PRE

### Make a new order

Restaurant

Pizza industrija

Choose...

Moj zavicaj

Pizza industrija

Pizza Vesuvio

Pizza Quattro Formaggi

Pizza Quattro Stagioni

Pizza kulen

Address

Gotham City, Bat cave

Additional Remark

Submit

## POSLE

# Make a new order

Restaurant

Moj zavicaj

Choose...

Moj zavicaj

Pizza industrija

I dobijamo gresku:

```
org.h2.jdbc.JdbcSQLException: Create breakpoint : This method is not allowed for a prepared statement; use a regular statement instead. [90130-200]
    at org.h2.message.DbException.getJdbcSQLException(DbException.java:505)
    at org.h2.message.DbException.getJdbcSQLException(DbException.java:429)
    at org.h2.message.DbException.get(DbException.java:205)
    at org.h2.message.DbException.get(DbException.java:181)
    at org.h2.message.DbException.get(DbException.java:178)
    at org.h2.jdbc.JdbcPreparedStatement.executeUpdate(JdbcPreparedStatement.java:322)
    at com.zaxxer.hikari.pool.ProxyStatement.executeUpdate(ProxyStatement.java:120)
    at com.zaxxer.hikari.pool.HikariProxyPreparedStatement.executeUpdate(HikariProxyPreparedStatement.java)
    at com.zuehlke.securesoftwaredevelopment.repository.OrderRepository.insertNewOrder(OrderRepository.java:56)
```

Kao rezultat, ne izvrsava se naredba!