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

Veganska Svinja

Amount

\$

Address Gotham City, Bat cave Additional Remark 'eganska Svinja', 999, 666); - Submit

Zastita

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

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

Kada izmenimo, dobijamo sledeci kod:

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

PRE

Make a new order

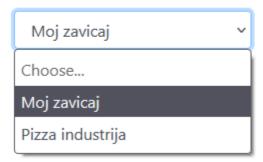
Restaurant	
Pizza industrija	~
Choose	
Moj zavicaj	
Pizza industrija	
Pizza Vesuvio	\$
Pizza Quattro Formaggi	•
Pizza Quattro Stagioni	\$
Pizza kulen	•
Address	
Gotham City, Bat cave	~
Additional Remark	
Submit	

^ 1

POSLE

Make a new order

Restaurant



I dobijamo gresku:

```
org.h2.jdbc.JdbcSQLNonTransientException Greate brekpoint: 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.get(DbException.java:205) 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:170) at org.h2.message.DbException.get(DbException.java:170) 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.java:120) at com.zaxxer.hikari.pool.HikariProxyPreparedStatement.java:120) at com.zaxxer.hikari.pool.HikariProxyPreparedStatement.java:120)
```

Kao rezultat, ne izvrsava se naredba!