



# Maintainability

# Today's Topics

- Sql Injection Demo
- Datamapper pattern
- Facade pattern

- Steal data
- Add
- Delete
- Change

# Preventing SQL injection

- Limit privileges
- Clean up the SQL input
- Prepared Statements



# Views



# Stored procedures



# Layered-architecture

# Stored procedure example 1

- Create stored procedure that retrieves all zip codes

```
DELIMITER //  
CREATE PROCEDURE GetAllZipcodes()  
BEGIN  
SELECT * FROM zipcodes;  
END //
```

Resource: <http://www.mysqltutorial.org/getting-started-with-mysql-stored-procedures.aspx>



# Stored procedure example 3

Call stored procedure from jdbc code:

```
...  
CallableStatement call = null;  
try {  
    call = con.prepareCall("{call GetAllZipcodes()}");  
    boolean hadResults = call.execute();  
    if (hadResults) {  
        rs = call.getResultSet();  
        while (rs.next()) {  
            city = rs.getString("city");  
            zip = rs.getInt("zip");  
            codes.add(new Zipcode(zip, city));  
        }  
    }  
}  
...
```

# Stored procedure parameters

```
DELIMITER //  
CREATE PROCEDURE GetZipcodes(IN cityName varchar(50))  
BEGIN  
SELECT * FROM zipcodes  
  where city like cityName;  
END //
```

## Call in JDBC code:

```
call = con.prepareCall("{call GetZipcodes(?)}");  
call.setString(1, city);
```