MODULE 2 DATABASE PROGRAMMING

Database Connectivity (JDBC)

TECH ELEVATOR
A Stride Company

YESTERDAY...

What is normalization?

How do we create a table in the database?

How do we drop a table in the database?

Gallery Customer History Form

Customer Name

Jackson, Elizabeth Phone (206) 284-6783
123 – 4th Avenue
Fonthill, ON
L3J 4S4

Purchases Made

Artist	Title	Purchase Date	Sales Price
03 - Carol Channing	Laugh with Teeth	09/17/2000	7000.00
15 - Dennis Frings	South toward Emerald Sea	05/11/2000	1800.00
03 - Carol Channing	At the Movies	02/14/2002	5550.00
15 - Dennis Frings	South toward Emerald Sea	07/15/2003	2200.00

The Gill Art Gallery wishes to maintain data on their customers, artists and paintings. They may have several paintings by each artist in the gallery at one time. Paintings may be bought and sold several times. In other words, the gallery may sell a painting, then buy it back at a later date and sell it to another customer.

ELEVATE YOURSELF

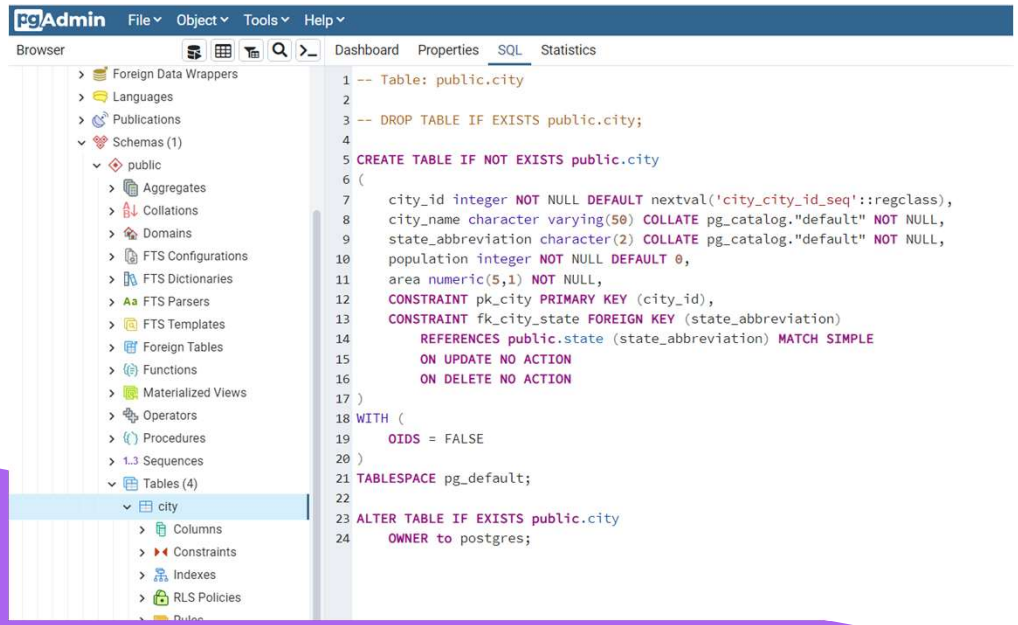
Persistent State

What is state?

Connecting to the database

- What have we used to connect to the database?

A client =>



Solving the database conundrum

- How many databases are there?
  - Microsoft SQL
  - MySQL
  - Oracle
  - PostGRE SQL
  - etc.

Needs for database access

- Database connection information
  - DataSource object;
- Client object
  - JdbcTemplate(dataSource);
- Set the command text
  - String sql = <command text variable>;
- Query the Database
  - queryForRowSet(sql,<parameter>);
- Get the data
  - Results.next()

Reading the data

- Get the data

```
SqlRowSet results = jdbcTemplate.queryForRowSet(sql, cityId);
```

- Read the data

```
while (results.next())
    {
    some code;
    }
```

Other Methods

- queryForObject(String,class,parameters)
  - Returns data of type <class>.
- update(String,parameters)
  - Updates or inserts into the database
  - No data is returned

DAO Pattern

- **Data Access Object (DAO)** design pattern encapsulates the details of persistent storage inside of classes whose only role is to store and retrieve data.

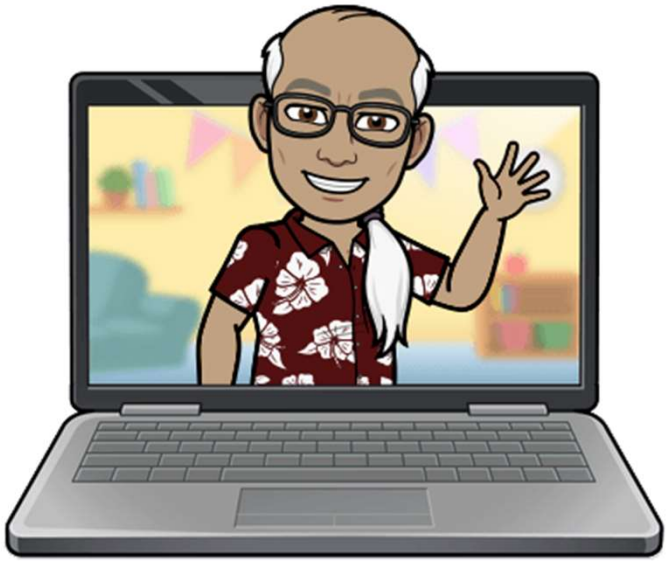
DAOs usually perform **CRUD** operations on domain objects.

- **C**reate
- **R**ead
- **U**pdate
- **D**elete

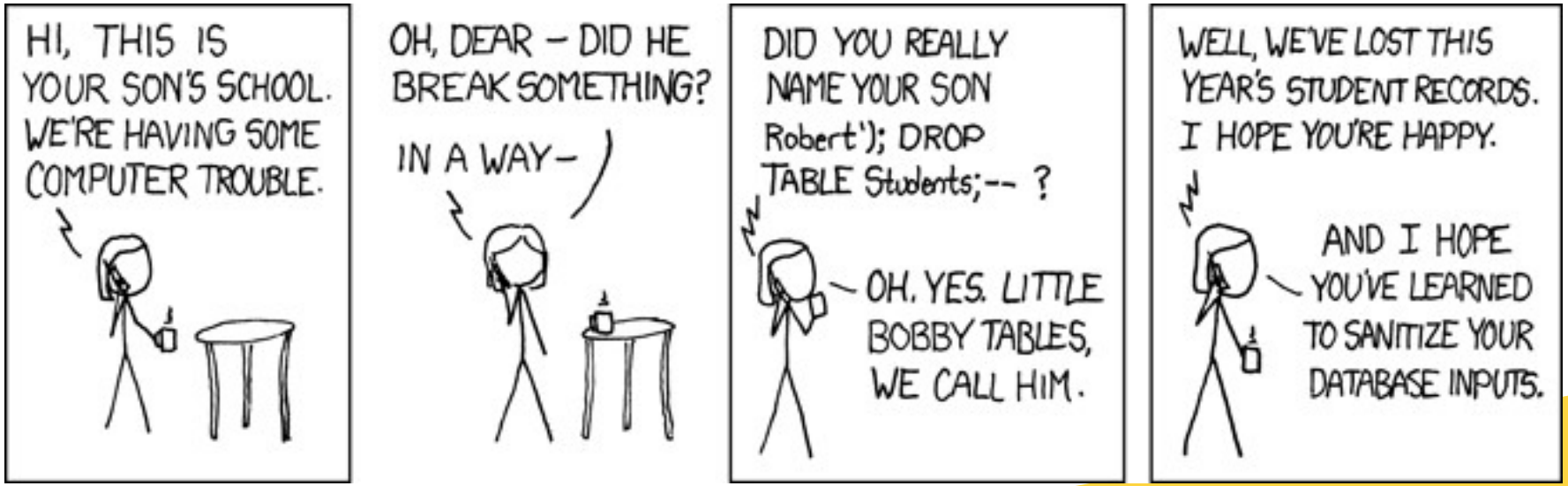
DAO pattern makes code **loosely coupled**

- Handle structure changes
- Change database technology

LET’S CODE!



Stop the bad guys.



SQL Injection

1. We ask the user for their input:
    1. Please enter your name:
    2. Henry Edwards
2. We use this input to query our database
    1. String nameEntered = scanner.nextLine();
    2. String sql = “SELECT * FROM message WHERE private = FALSE AND sender_name =“‘ + nameEntered + “ ‘ ORDER BY create_date DESC”
3. We think that should be:
    1. SELECT * FROM message WHERE private = FALSE AND sender_name =‘Henry Edwards’ ORDER BY create_date DESC
4. Riiight?

SQL Injection

1. We ask the user for their input:
    1. Please enter your name:
    2. Robert'; Drop TABLE Students;--
2. We use this input to query our database
    1. String nameEntered = scanner.nextLine();
    2. String sql = "SELECT * FROM message WHERE private = FALSE AND sender_name ="" + nameEntered + " ' ORDER BY create_date DESC"
3. We think that should be:
    1. SELECT * FROM message WHERE private = FALSE AND sender_name ='**Robert'; Drop TABLE Students;--** ORDER BY create_date DESC
4. Ooops.

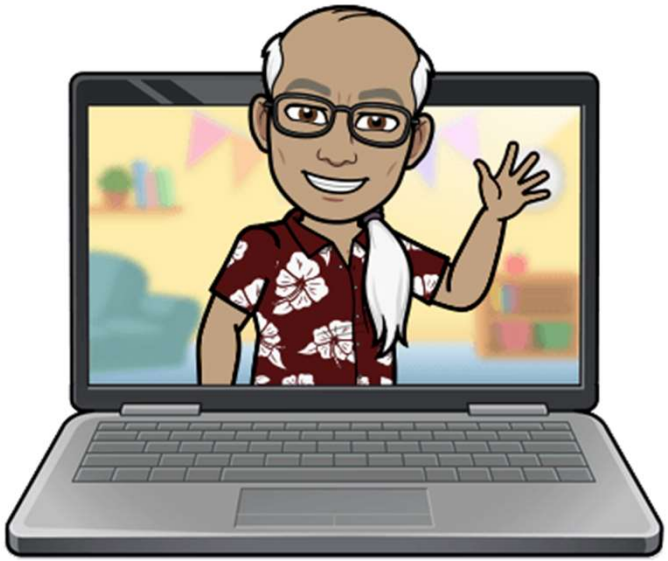
SQL Injection

1. We ask the user for their input:
    1. Please enter your name:
    2. ‘ OR ‘1’=‘1
2. We use this input to query our database
    1. String nameEntered = scanner.nextLine();
    2. String sql = “SELECT * FROM message WHERE private = FALSE AND sender_name =“‘ + nameEntered + “ ‘ ORDER BY create_date DESC”
3. We think that should be:
    1. SELECT * FROM message WHERE private = FALSE AND sender_name =‘‘ **OR ‘1’=‘1**’ ORDER BY create_date DESC
4. Ooops.

Practice Safe Computing

- **Parameterized Queries:** If this is done consistently, SQL injection will not be possible
- **Input Validation:** Only allow certain values to be accepted. (Many of you did this in your Vending Machine)
- **Limit Database User Privileges**: A web application should always use a database user to connect to the database that has as few permissions as necessary. Never a good idea to use an admin's account

LET’S CODE!



WHAT QUESTIONS DO YOU HAVE?

Reading for Tonight:

DAO Part 2