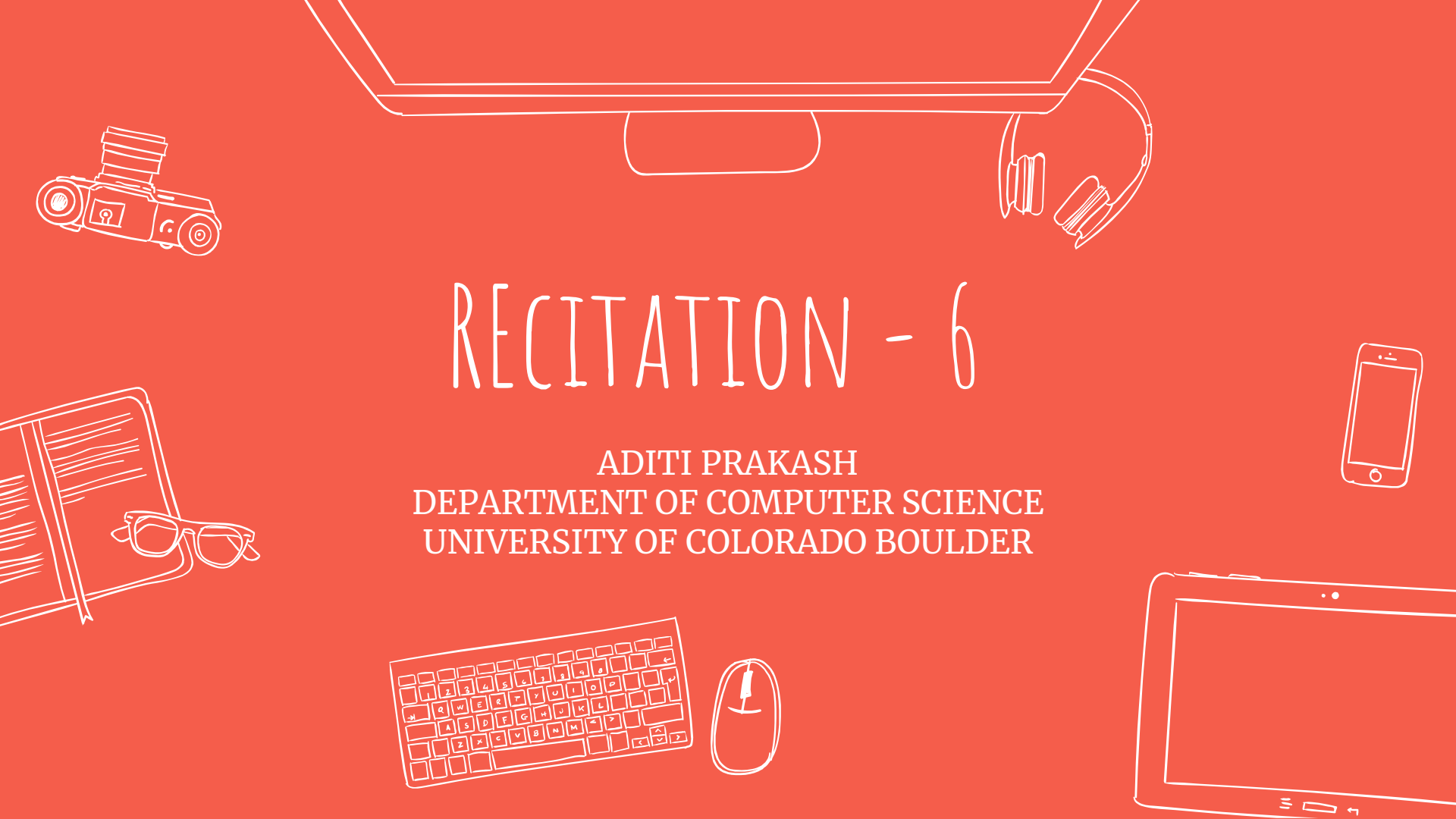
Recitation - 6

ADITI PRAKASH
DEPARTMENT OF COMPUTER SCIENCE
UNIVERSITY OF COLORADO BOULDER



SQL

What is SQL?

- Structured Query Language
- Query and edit database
- RDBMS
- Some Operations: Create, select, insert, update, delete, drop

Basics

- Not case-sensitive
- Semi-colon

Know these words

Table : database(DB)

Select: extract from DB

Update: update DB

Tuple: record

Delete: Delete record from DB

Insert into: insert new data into DB

Fields:column

Create table: create a new database

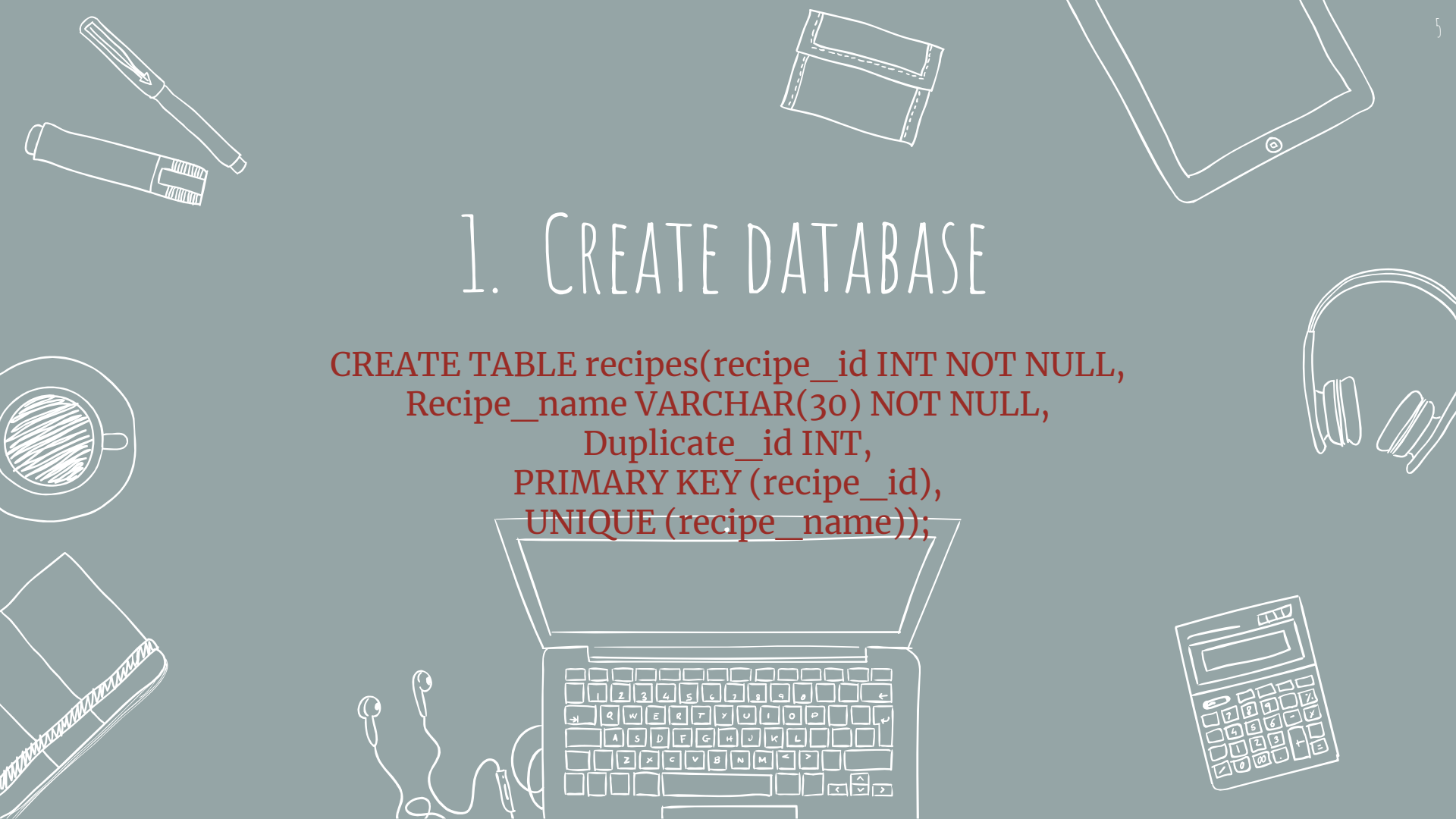
Alter table: modifies DB

Drop table: deletes a table


LETS CODE
HTTP://SQLFIDDLE.COM/
MacBook Air

1. Create database

```
CREATE TABLE recipes(recipe_id INT NOT NULL,
Recipe_name VARCHAR(30) NOT NULL,
Duplicate_id INT,
PRIMARY KEY (recipe_id),
UNIQUE (recipe_name));
```



2. INSERT

```
INSERT INTO recipes(recipe_id, recipe_name,duplicate_id)
VALUES
(1, “Tacos”,1),
(2,”Pasta”,1),
(3,”Soup”,2);
```

3. QUERY DATABASE

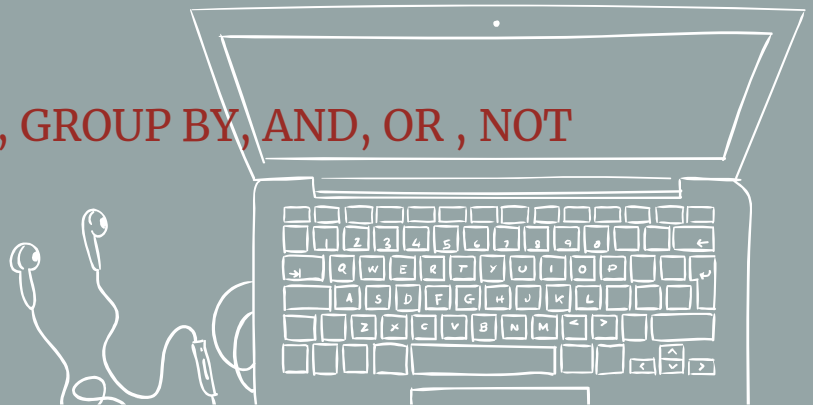
SELECT * from recipes;

SELECT * from recipes where recipe_name = “Tacos”;

SELECT recipe_id from recipes;

SELECT DISTINCT duplicate_id from recipes;

Others:
ORDER BY, GROUP BY, AND, OR , NOT



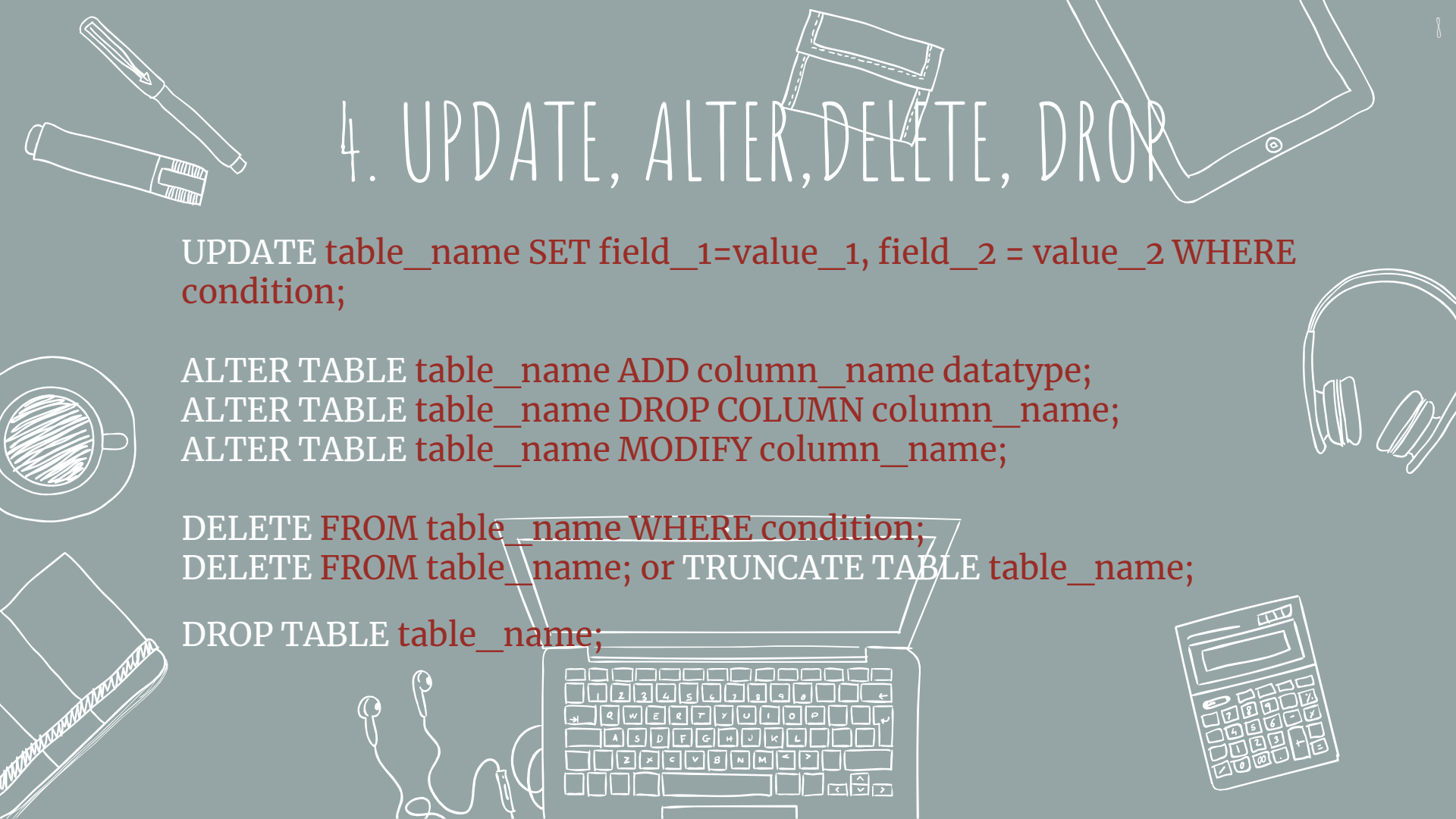
4. UPDATE, ALTER, DELETE, DROP

UPDATE table_name SET field_1=value_1, field_2 = value_2 WHERE condition;

ALTER TABLE table_name ADD column_name datatype;
ALTER TABLE table_name DROP COLUMN column_name;
ALTER TABLE table_name MODIFY column_name;

DELETE FROM table_name WHERE condition;
DELETE FROM table_name; or TRUNCATE TABLE table_name;

DROP TABLE table_name;



5. JOINS

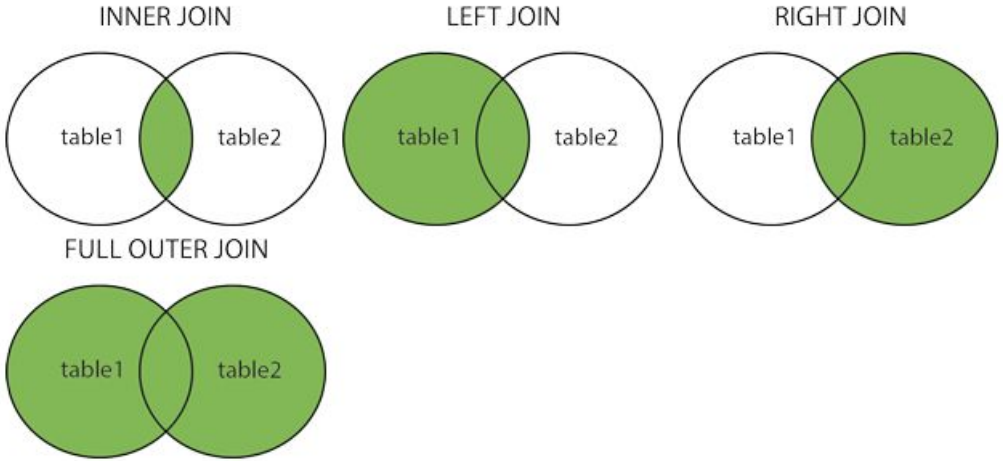
Combines rows from 2 or more tables based on a related column between them.

OrderID	CustomerID	OrderDate
10308	2	1996-09-18
10309	37	1996-09-19
10310	77	1996-09-20

CustomerID	CustomerName	ContactName	Country
1	Alfreds Futterkiste	Maria Anders	Germany
2	Ana Trujillo Emparedados y helados	Ana Trujillo	Mexico
3	Antonio Moreno Taquería	Antonio Moreno	Mexico

```
SELECT Orders.OrderID, Customers.CustomerName, Orders.OrderDate
FROM Orders INNER JOIN Customers ON
Orders.CustomerID=Customers.CustomerID;
```

- **(INNER) JOIN**: Returns records that have matching values in both tables
- **LEFT (OUTER) JOIN**: Returns all records from the left table, and the matched records from the right table
- **RIGHT (OUTER) JOIN**: Returns all records from the right table, and the matched records from the left table
- **FULL (OUTER) JOIN**: Returns all records when there is a match in either left or right table



6. UNIONS

Combines result set of two or more select statements:

- Each SELECT statement within UNION must have the same number of columns
- The columns must also have similar data types
- The columns in each SELECT statement must also be in the same order
- Returns distinct results

```
SELECT City FROM Customers
UNION
SELECT City FROM Suppliers
ORDER BY City;
```

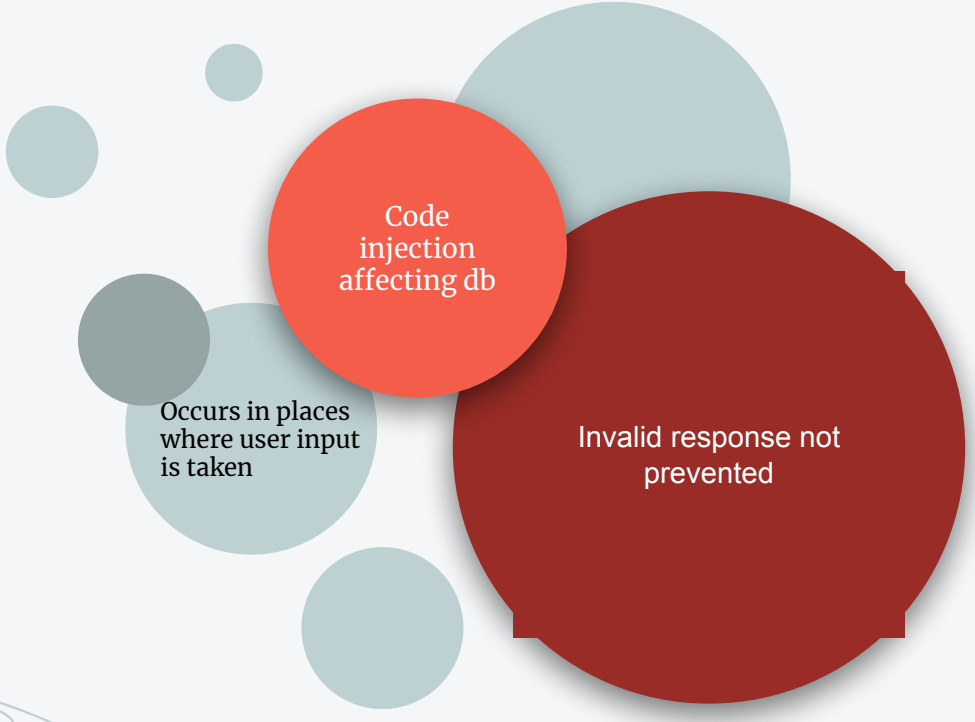
Below is a selection from the "Customers" table:

CustomerID	CustomerName	ContactName	Address	City	PostalCode	Country
1	Alfreds Futterkiste	Maria Anders	Obere Str. 57	Berlin	12209	Germany
2	Ana Trujillo Emparedados y helados	Ana Trujillo	Avda. de la Constitución 2222	México D.F.	05021	Mexico
3	Antonio Moreno Taquería	Antonio Moreno	Mataderos 2312	México D.F.	05023	Mexico

And a selection from the "Suppliers" table:

SupplierID	SupplierName	ContactName	Address	City	PostalCode	Country
1	Exotic Liquid	Charlotte Cooper	49 Gilbert St.	London	EC1 4SD	UK
2	New Orleans Cajun Delights	Shelley Burke	P.O. Box 78934	New Orleans	70117	USA
3	Grandma Kelly's	Regina Murphy	707 Oxford	Ann	48104	USA

SQL INJECTION



COMMON MISTAKES

- SELECT * FROM Users WHERE UserId = 105 OR 1=1;
- sql = 'SELECT * FROM Users WHERE Name ="' + uName + '" AND Pass ="' + uPass + '"'
  - SELECT * FROM Users WHERE Name ="" or ""="" AND Pass ="" or ""=""
- txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
  - SELECT * FROM Users WHERE UserId = 105; DROP TABLE Suppliers;

Protect with SQL parameters

- SQL parameters are values that are added to an SQL query at execution time, in a controlled manner.

ASP.NET

- txtUserId = getRequestString("UserId");
  txtSQL = "SELECT * FROM Users WHERE UserId = @0";
  db.Execute(txtSQL,txtUserId);

Resources

Linux installation of Wireshark
https://www.youtube.com/watch?v=VcLrcnx8umM

SQL basics link
https://www.w3schools.com/sql/

More about SQL injection
https://portswigger.net/web-security/sql-injection
https://www.veracode.com/security/sql-injection