COMP6443 25T1 - Week 4

SQL and Injection

TrashPanda, 11th March 2025

What’s happening in Cyber Security?

Any Questions?

https://questions.quoccacorp.com

Some notes from Tutors

- We are considering enumeration and brute force to be different things
  - You are allowed to brute force offline

Last Week in Review

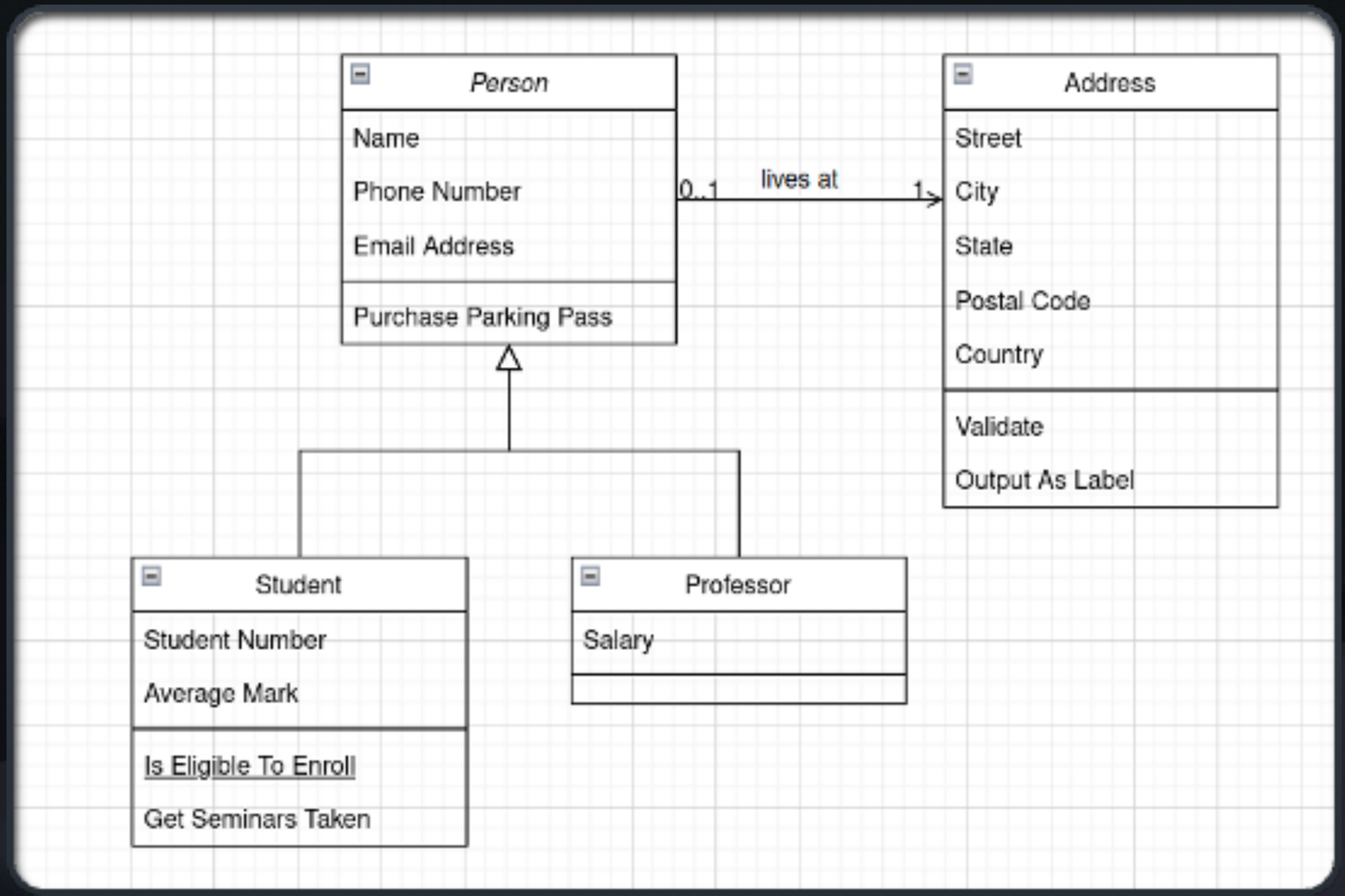
Content

- We started with databases!
- We can interface with a SQLite3 database via python and flask

Stepping Back

What does a database look like?

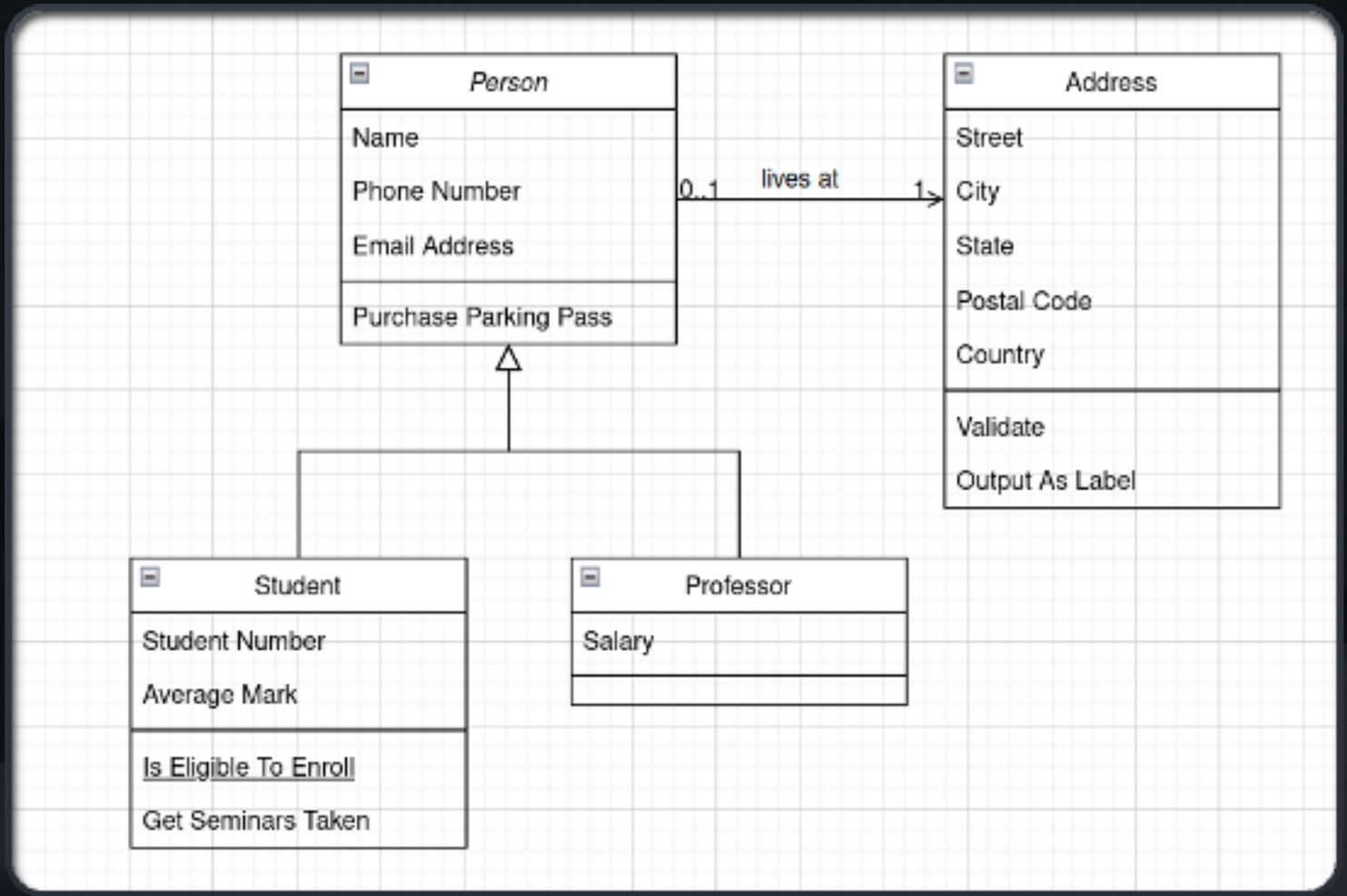
- Bunch of tables with columns
- These columns can point to each other between tables, hence the relations
- There are many types of relations
  - One to one
  - One to many
  - Many to one
  - Many to Many



Stepping Back

What does a database look like?

- Each entry usually has a unique identifer, known as a primary key (or sometimes primary key set)
- Foreign keys are what enables pointing across tables
- You can have other restrictions on data like “NOT NULL” where an entry MUST exist



What's that in code?

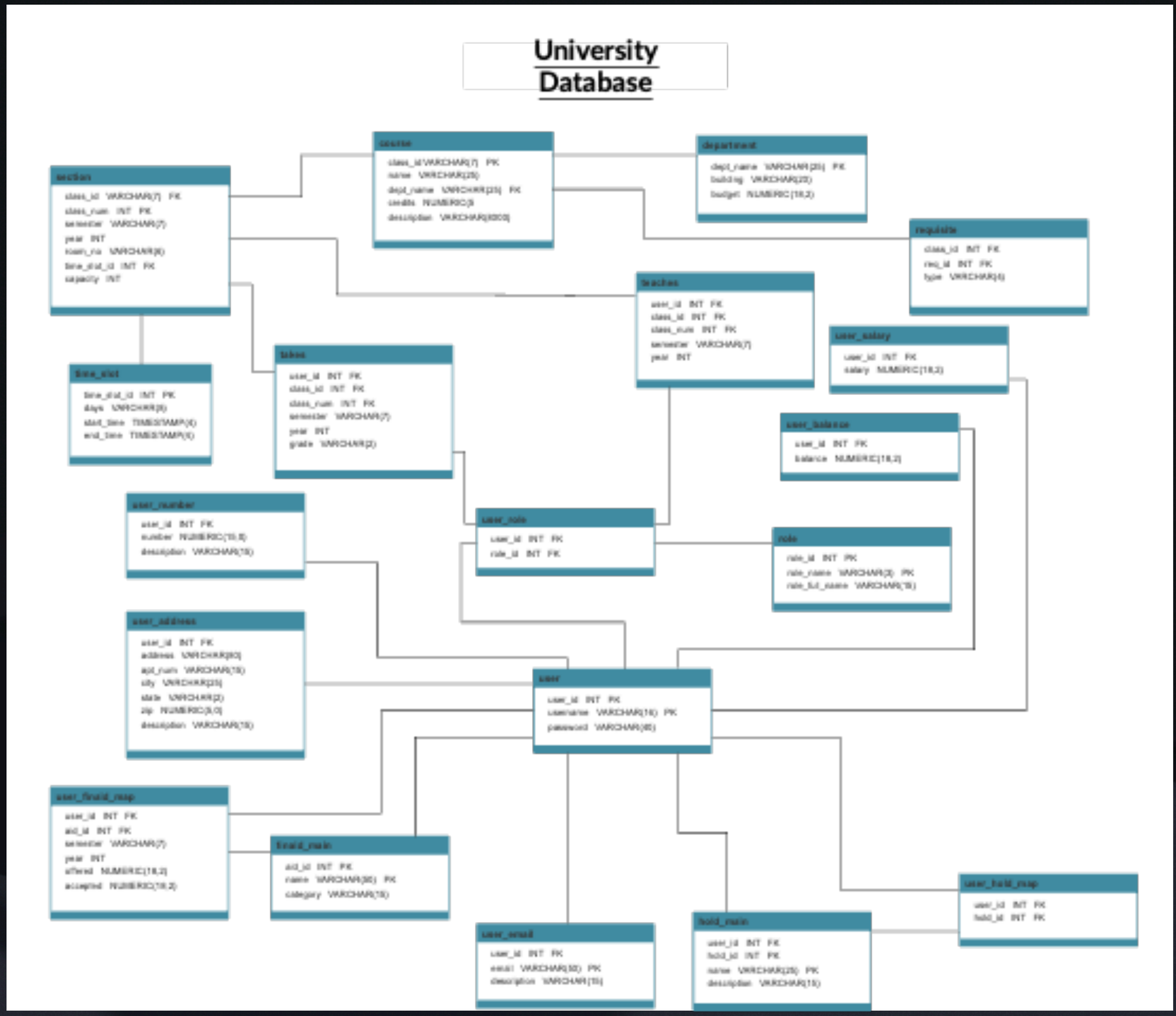
SQL

```
CREATE TABLE person (
  name TEXT,
  phone_number INTEGER,
  email_address TEXT
);

CREATE TABLE address ( ...
```

What about a real database?

They can get pretty complicated...



SQL Commands

- SELECT – Selecting from a table
- INSERT – Putting into a table
- UPDATE – Updating an entry
- DELETE – Deleting an entry
- JOIN – Combining two tables into one big table – more columns
- UNION – Combining two select queries into one long table – More rows
- WHERE – Add a constraint to a query where the clause is true
- LIMIT – Limit to only N results

Let’s Build It!

Injection

SQL Injection

Mixing data and control

We are able to insert CONTROL characters into our DATA

This is referred to as **INJECTION**

Example:

SELECT username FROM users WHERE

username == 'request.data["username"]' AND

Password == 'request.data["password"]'; -- I'll implement hashing eventually...

INJECTING THE CODE

```
SELECT USERNAME FROM USERS WHERE
    USERNAME == 'ADMIN' AND
    PASSWORD == '1' OR '1'='1';
```

Demos!

Schema Dumping...

Dumping the schema

- You can get information about the database from the meta tables
  - SELECT * FROM information_schema.tables;
- These are consistent for all MySQL instances but are different for different SQL providers – PostgreSQL, SQLite, MSSQL, etc.

- See more: https://dev.mysql.com/doc/mysql-infoschema-excerpt/8.0/en/information-schema.html

Remediation

Prepared Statements and Paramaterised Queries

- Forces the database to expect a specific type of query by creating a model
- If the query received is outside the expected mode, return an error

- Paramterised queries are similar except they’re defined in the SQL database instead of the querying code.

```
query = """Update employee set Salary = %s where id = %s"""
tuple1 = (8000, 5)
cursor.execute(query, tuple1)
```

Other Methods

These work sometimes but there’s always bypasses

- Escape all control characters
  - This is generally good practice regardless, but there's always a way around it

- Allow Listing
  - This is where you explicitly define what tables are allowed to be viewed
    - E.g. Granting select permissions for a user on the courses table, but not on the grades table
  - Not always helpful as you can leak data within the same table – user passwords for example
  - Always a way around the whitelisting

Real world examples of SQLi

- **Tesla vulnerability**—in 2014, security researchers publicized that they were able to breach the website of Tesla using SQL injection, gain administrative privileges and steal user data.
- **Fortnite vulnerability**—Fortnite is an online game with over 350 million users. In 2019, a SQL injection vulnerability was discovered which could let attackers access user accounts. The vulnerability was patched.
- **Turkish government**—another APT group, RedHack collective, used SQL injection to breach the Turkish government website and erase debt to government agencies.
- **7-Eleven breach**—a team of attackers used SQL injection to penetrate corporate systems at several companies, primarily the 7-Eleven retail chain, stealing 130 million credit card numbers.
- https://brightsec.com/blog/sql-injection-attack/

SQLi to RCE

It happens!

- Some SQL providers will allow you to create a file by using the "into_outfile" command
- Which means you can run a select on a static string and put that into a file. If you can access the file, sometimes you can get RCE.
- https://kayran.io/blog/web-vulnerabilities/sqli-to-rce/

- Or you could just run the "Give me RCE" command. Yes. That's a thing.
- https://learn.microsoft.com/en-us/sql/relational-databases/system-stored-procedures/xp-cmdshell-transact-sql?view=sql-server-ver16