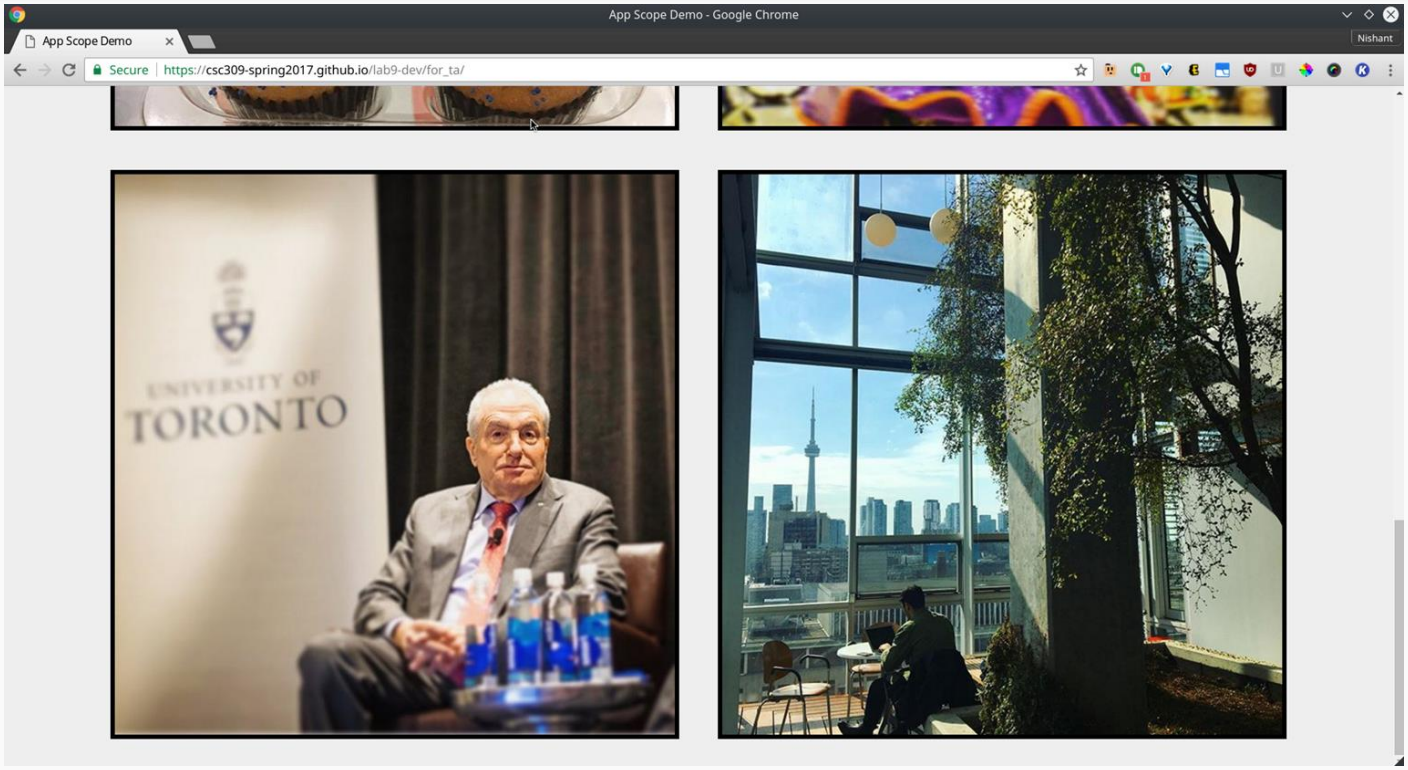
CSC309 - Winter 2017

Lab 10 - Web Security

Lab 9 : Review

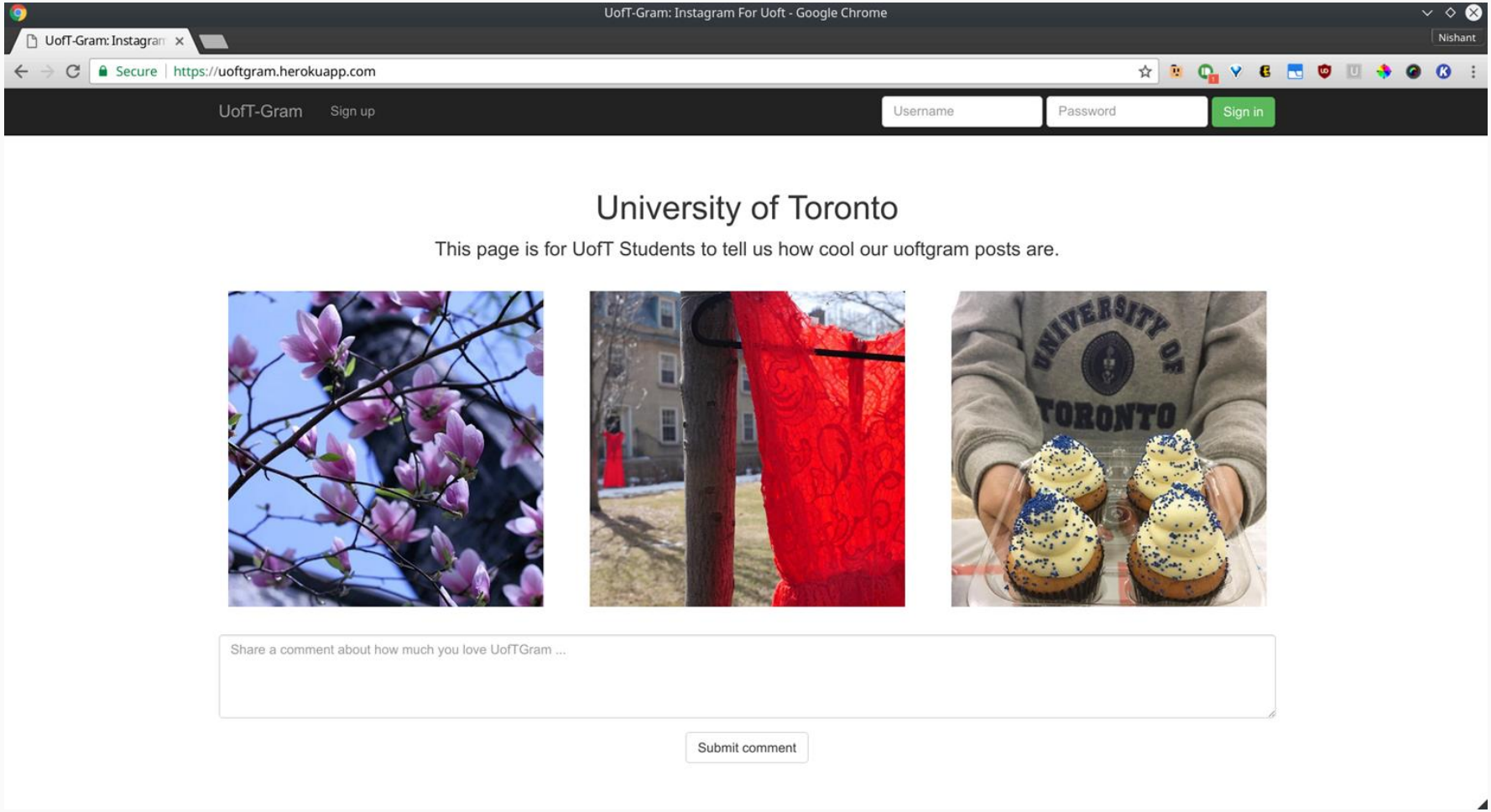


- Final Demo: https://csc309-spring2017.github.io/lab9-dev/for_ta/
- Final JS: https://csc309-spring2017.github.io/lab9-dev/for_ta/app.js
- Short URL: `https://goo.gl/WRIfro`

PLEASE DISCUSS WITH YOUR TA IF SOMETHING DOES NOT WORK

TAs Please Go Through The app.js code once.

Web Security



We Built Something Cool, Now we want you to break it.

There Are Four Vulnerabilities

These Include:

- Cross-Site Scripting Vulnerability (XSS)
- Cross-Site Request Forgery (CSRF)
- SQL Injections

SQL Injections

- The SQL injection vulnerability is (probably) the most challenging to exploit
  - This will be considerably easier when you can see the source in the latter part of the lab
- Start with trying to find the other vulnerabilities
  - None of the vulnerabilities depend on each other -- each can be exploited without having found any of the others
  - Nevertheless, I'm going to show you two quick things that will help when trying to do SQL injection

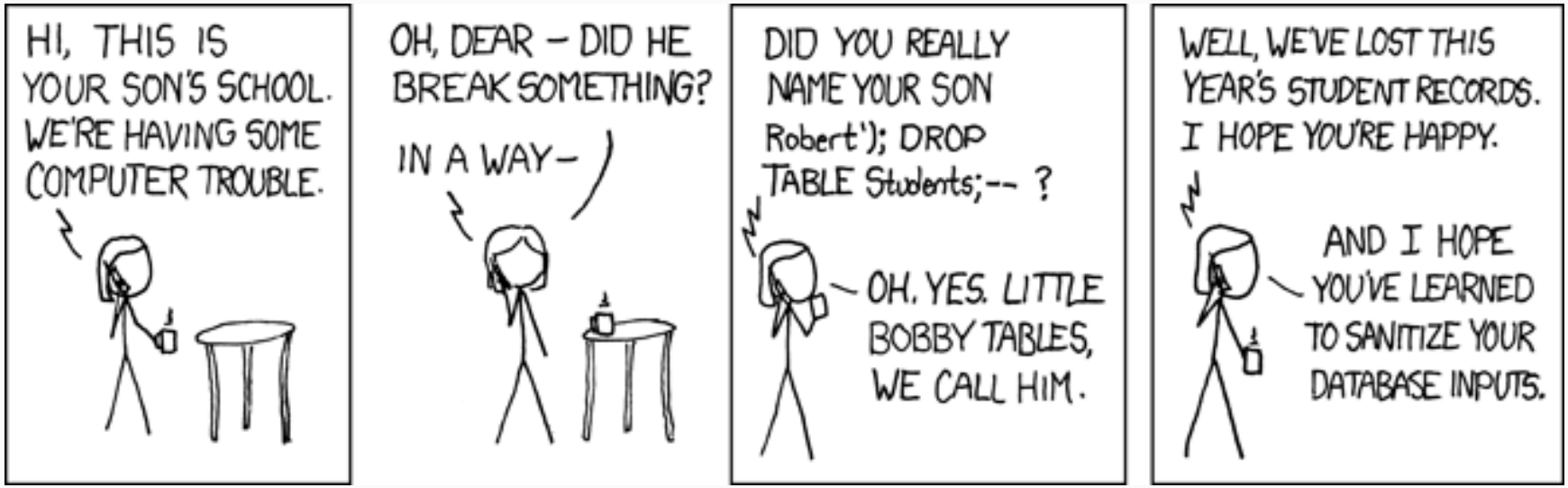
SQL Injections

- UNION SQL queries are super neat
- Imagine: `SELECT id, username, password, is_admin FROM users WHERE username = 'foo'`
  - Assuming foo is a real user who is not an admin with user ID = 1, this returns (1, foo, <hashed password>, 0), which is only one row
- UNION: take union of results from two completely different queries, provided they have same number of columns
  - Example:
    ```
    SELECT id, username, password, is_admin
    FROM users WHERE username = 'foo'
    UNION
    SELECT 500, 'Jeff', '<some password hash>', 1
    ```
  - Returns two rows: `((1, foo, <hashed password>, 0), (500, Jeff, <some password hash>, 1))`

SQL Injections

- To do password hashing, we're using bcryptjs: https://www.npmjs.com/package/bcryptjs
- SQL comments can be useful when you're trying to be naughty:
  - `SELECT col ... -- everything after these two hyphens is a comment`
  - `SELECT username, password WHERE username = 'foo'`
  - `Instead of foo, what if username is someone' OR is_admin = 1?`
- Then the query is `SELECT username, password WHERE username = 'someone' OR is_admin = 1'`
  - You still have that pesky closing quote that makes this query invalid
- But if you append -- to the username you enter, you comment out the closing quote

Other Vulnerabilities



- Other Hints are provided along with the readme code.
- Go through them and try hacking the application.

Quiz Time