Problem 6: TigerHub 2.0

By Henry Tang

The key to this problem was realizing that the second page (the forgot password page) had a SQL Injection vulnerability, while the login page did not. Typically, when presented with an SQL injection vulnerability, you will try to get the query to return all the data in a database, as opposed to just the data stored in one row. However, in this case, the query was the following

```
SELECT COUNT(1)
FROM users
WHERE username = \‘%s\’
```

Thus, you are only able to figure out if a certain username exists or not in the database. However, we can exploit this to our advantage. Consider entering the following text into the Forgot Password page:

```
tygasan’ AND substr(password,1,1) = ‘2
```

The resulting query that the database server executes is

```
SELECT COUNT(1)
FROM users
WHERE username = ‘tygasan’ AND substr(password,1,1) = ‘2’
```

Let’s see what this does. This query returns 1 if there exists a row where the username is `tygasan` and the first character of the password is 2. When we try this on the website, we are presented with the message that the email does exist in the database. Thus, we can conclude that the first character of the password is 2. Then, we can test for the second character in the same way, and so forth. Another useful trick was to use the injection vulnerability to first nail down the length of the password. For example, entering

```
tygasan’ AND length(password) < 10 AND ‘1’ = ‘1
```

returns the green “a password reset has been sent” message, and lets us know that the password is less than ten characters. The final credentials were

```
username: tygasan       password: 27638       grades: B+, C, A, C-, B-, A-
```

(It goes without saying that we don’t actually know who Tyga San is, how they identify, and what his/her/their grades are. The grades were generated at random.)

Plaudits:

- Congratulations to Ilya Chugonov (grad) who was head and shoulders above the rest and solved the problem in an impressive 47 minutes!
- Congratulations to Charles Zhao '21 and Geoffrey Mon '21 for being the first UG team to solve this problem! They were the second team overall to solve the problem, which they did in 148 minutes.