cs3235:8: - Laboratory #8 for 23rd of October, 2019

To get information useful for this laboratory, you could look at `http://www.w3schools.com/sql/`. Again, the laboratory is very easy, and I suggest you use the extra time to meet up with your project group members, and work on your project. The laboratory will be open until Sunday evening.

1 Lab 8, part 1: SQL injection

In this laboratory, you will be investigating SQL injection attacks. Your final goal will be to change your grade for Lab 8 part 1. It is currently 0.

Open the web browser and go to

`https://hugh.comp.nus.edu.sg/cs3235/lab8/gradeslab8-1.php`

to see an application which allows the office staff at NUS to see your current gradings. There is a mindless interface that asks them to enter their userID and password, and then put in your ID, and then it will return your marks so far. This web page accesses your grade information in a SQL (actually mySQL) database, and unfortunately was written by someone with a brain the size of a pea[1]. As a result, the web page will be open to SQL injections.

I have put in a bit of debugging for you, which actually shows you the SQL command that will be executed when the office staff access your grades, although of course this does not normally happen in practice. I have also set things up so that your usercode and password allows you to pretend you are part of the office staff.

The SQL commands you might need might include ones like:

```
SELECT `field` FROM `database`.`tablename` WHERE field='value';
UPDATE `database`.`tablename` SET `field1` = 'value' WHERE field2 = 'value';
```

Experiment with the mindless interface, until you can see everyone else's marks and also change your own mark. Please do not change anyone else's mark, or do anything malicious to the database[2]. Please give yourself whatever mark you believe that you deserve.

[1] Me, once again.

[2] No DROP TABLES etc.

2 Lab 8, part 2: (individual homework question) Rainbow table chains

In class, Hugh briefly described Rainbow tables. When generating rainbow tables for passwords, long chains of interleaved hashes and candidate passwords are generated. At the end of computing each chain, we discard all the intermediate values, and only keep the first and last element. Explain in your own words why we keep the *first* element.

Access the cs3235 grading website, and enter your username, password, and the answer to this questionr:

`https://hugh.comp.nus.edu.sg/cs3235/lab8/gradeslab8-2.php`

3 Lab 8, part 3: (individual homework question) Reversible mappings

A good block cipher with blocks containing n-bits should be able to reversibly map any n-bit value to another n-bit value (even to itself perhaps). Answer the following two questions:

- How many different mappings are possible with an n-bit block cipher?
- Compare your answer above to the number of mappings available with DES or AES, and explain the difference, if any.

Access the cs3235 grading website, and enter your username, password, and the answer to both parts of this question:

`https://hugh.comp.nus.edu.sg/cs3235/lab8/gradeslab8-3.php`

4 Lab 8, part 4: (individual homework question) Bad guys in-the-middle

Imagine that you are in the ITSEC/OS laboratory, and about to encrypt a message to your friend "Eric the half-a-bee", using Eric's public key. You access Eric's public key from his web site `eric.org`.

- Explain in detail how a man-in-the-middle attack might be done, if there is a *malicious* machine through which your packets pass. Assume that your message still gets to Eric unchanged, but that Harry-the-hacker will have read it. You start the process by sending a packet to `eric.org` asking for Eric's public key.
- Give two ways that Harry-the-hacker in the ITSEC/OS lab may be able to make your messages to and from `eric.org` go via his machine `harry`.

Access the cs3235 grading website, and enter your username, password, and the answer to both parts of this question:

`https://hugh.comp.nus.edu.sg/cs3235/lab8/gradeslab8-4.php`