

SWS3011 – DOTA Defense of the Ancients

Lab 4

Shen Jiamin

Part 1: SQL Injection

- The SQL statement is constructed via string concatenation.

```
SELECT `marks` FROM `test`.`mrks` WHERE userName='???'
```

- ``jiamin`` will turn to

```
SELECT `marks` FROM `test`.`mrks` WHERE userName='jiamin'
```

- ``a' or '1'='1`` will turn to

```
SELECT `marks` FROM `test`.`mrks` WHERE userName='a' or '1'='1'
```

- What about this one?

```
jiamin'; SELECT * FROM `test`.`mrks` WHERE '1' = '1
```

- Please don't try to manipulate other's grades.
 - In the event of an accidental manipulation, please alert your TA.

Part 2: XSS

- Use the **secondary password** you were sent in the email.
- You may post this script on your page:

```
<script> alert(1); </script>
```

The script will be executed when someone visit your page.

- When visiting your comment page URL1, visitors shall be automatically redirected to user testx's page at URL2.
 - The URL1 is embedded into URL2.
 - URL1 should be posted on testx's comment page.

Tips

- Part 1
 - Please don't try to manipulate other's grades.
 - In the event of an accidental manipulation, please alert your TA.
- Part 2
 - Work in pairs.
 - Use the **secondary password** you were sent in the email.
- Part 3
 - The documentation is in the script, starting from line 367.
 - <https://www.cloudflare.com/en-gb/learning/ddos/ddos-attack-tools/slowloris/>