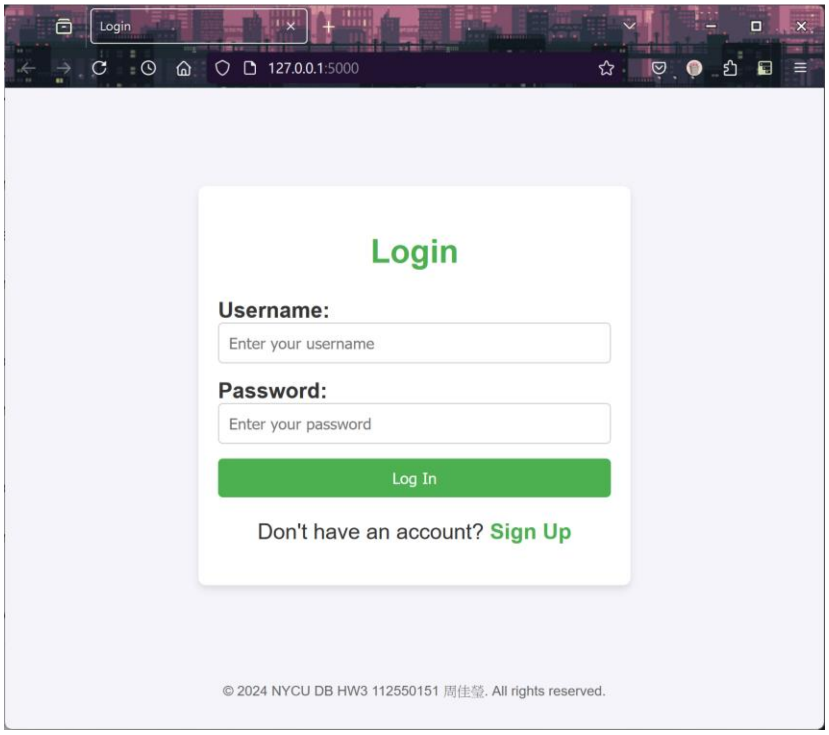
Homework 3 Report 112550151 周佳瑩

1. Screenshot of Footers (5%)



Login

Username:

Enter your username

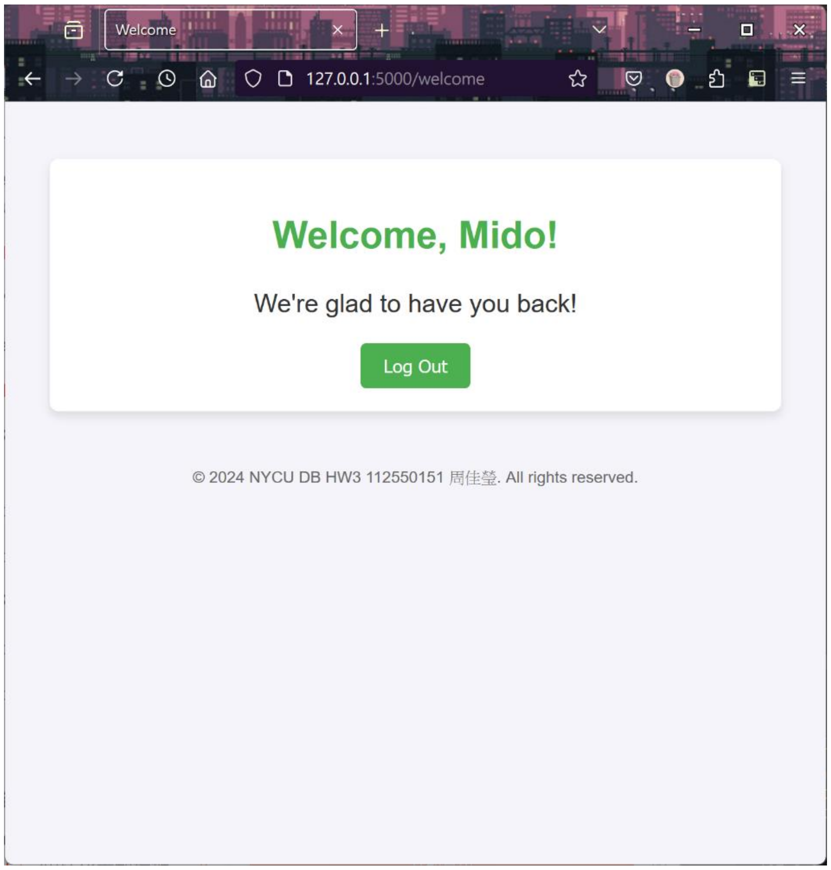
Password:

Enter your password

Log In

Don't have an account? Sign Up

© 2024 NYCU DB HW3 112550151 周佳瑩. All rights reserved.

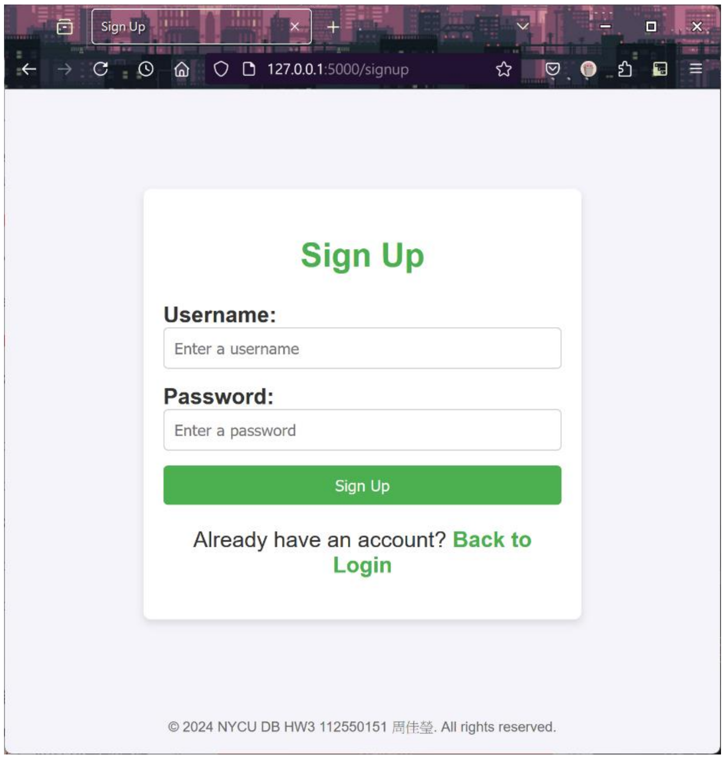


Welcome, Mido!

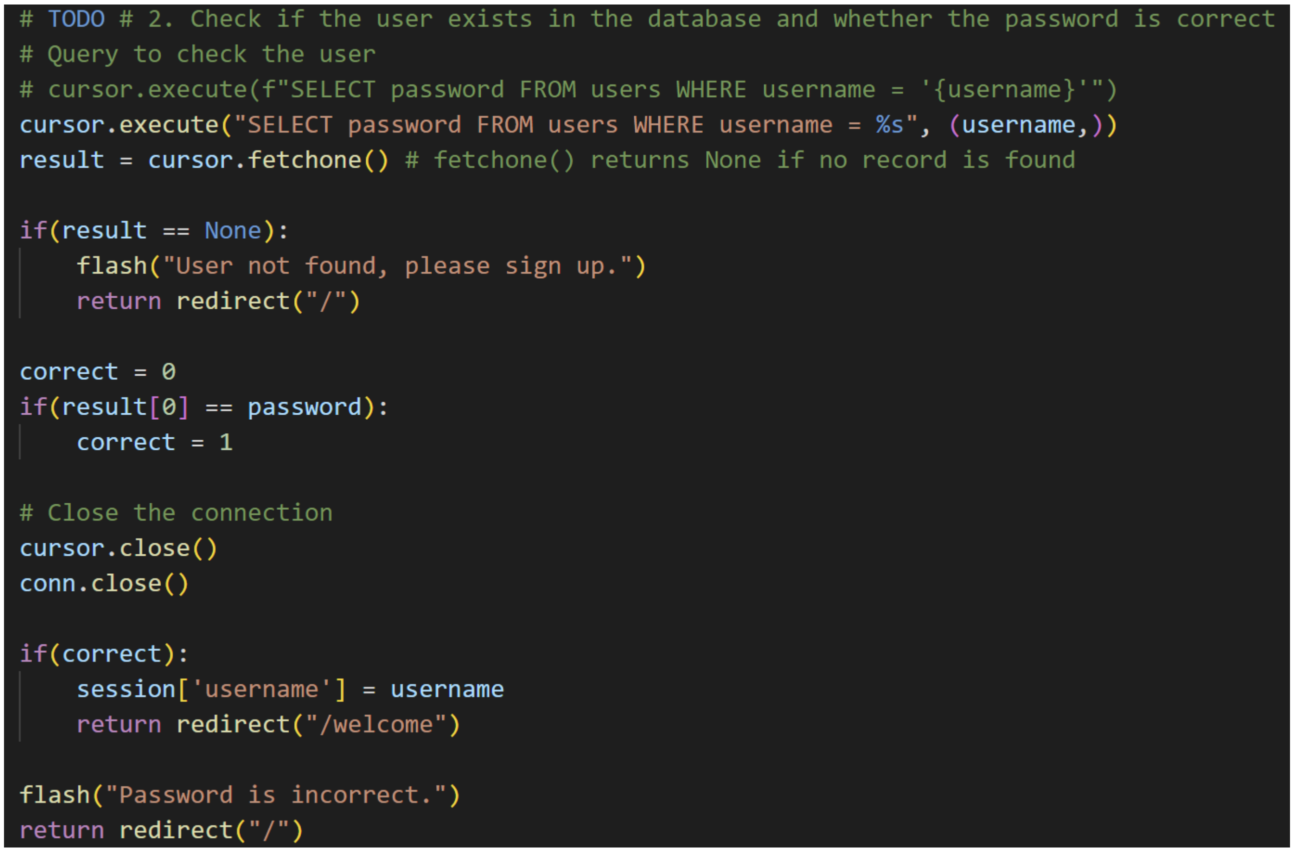
We're glad to have you back!

Log Out

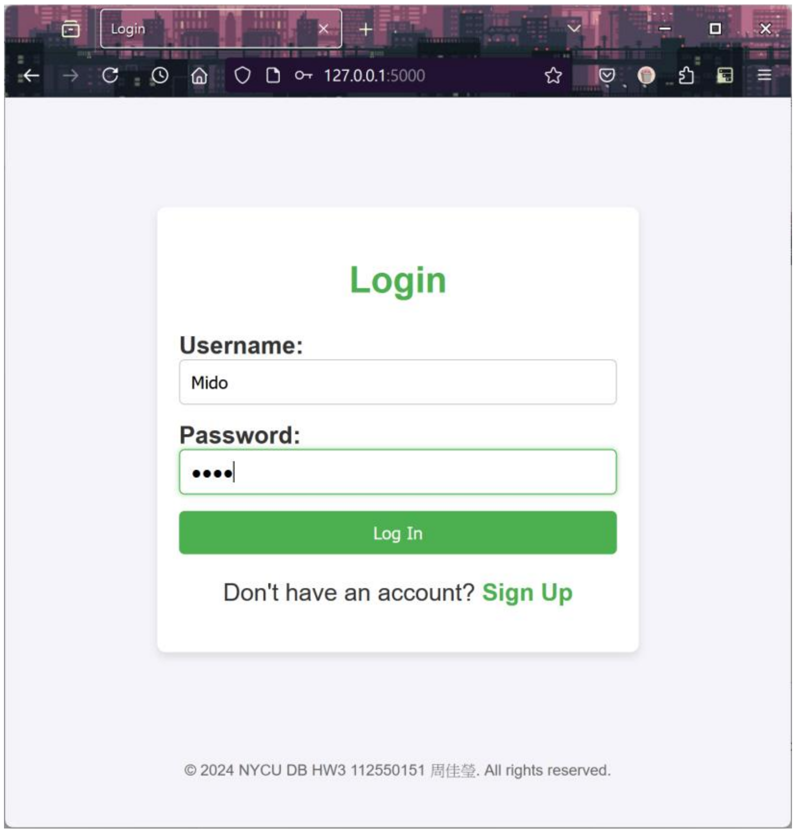
© 2024 NYCU DB HW3 112550151 周佳瑩. All rights reserved.


Sign Up
127.0.0.1:5000/signup
Sign Up
Username:
Enter a username
Password:
Enter a password
Sign Up
Already have an account? Back to Login
© 2024 NYCU DB HW3 112550151 周佳瑩. All rights reserved.

2. Screenshot and Explanation of Login Function (5%)
   If no record is found and fetchone() returns None, the user has to retype the username and password. Correct is used to check if the password is correct. If it is, the user is redirected to the login page. If the password is incorrect, the user has to retype the username and password.



```python
# TODO # 2. Check if the user exists in the database and whether the password is correct
# Query to check the user
# cursor.execute(f"SELECT password FROM users WHERE username = '{username}'")
cursor.execute("SELECT password FROM users WHERE username = %s", (username,))
result = cursor.fetchone() # fetchone() returns None if no record is found

if(result == None):
    flash("User not found, please sign up.")
    return redirect("/")

correct = 0
if(result[0] == password):
    correct = 1

# Close the connection
cursor.close()
conn.close()

if(correct):
    session['username'] = username
    return redirect("/welcome")

flash("Password is incorrect.")
return redirect("/")
```



Login

Username:

Mido

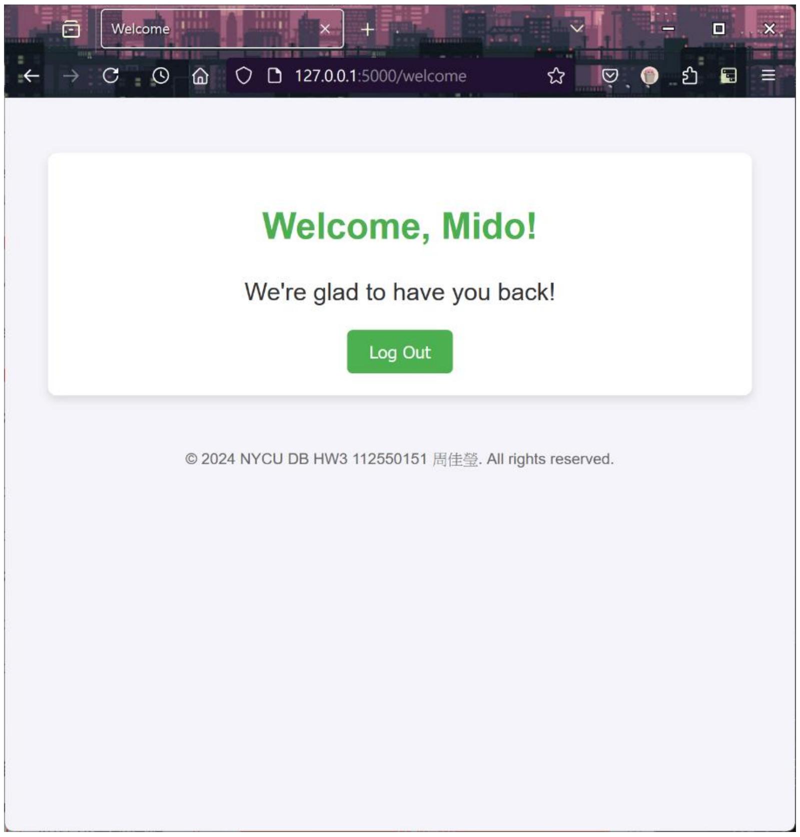
Password:

••••

Log In

Don't have an account? Sign Up

© 2024 NYCU DB HW3 112550151 周佳瑩. All rights reserved.



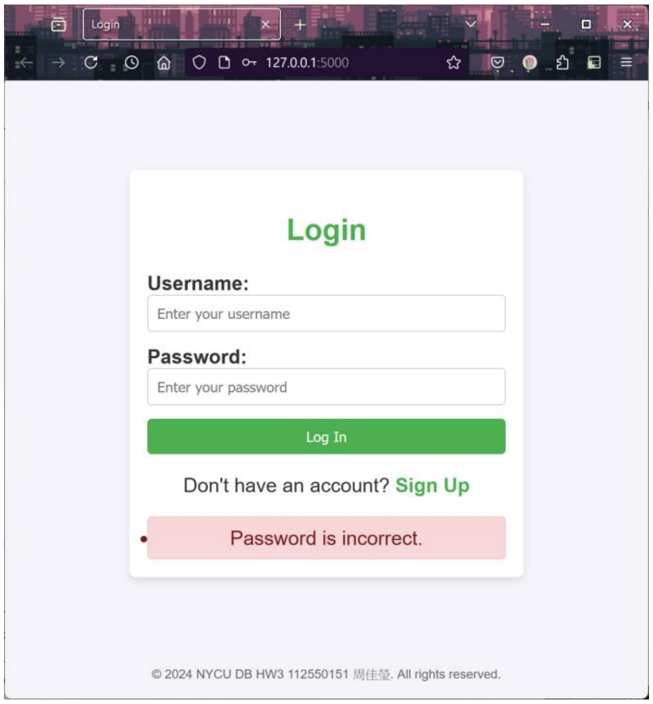
Welcome, Mido!

We're glad to have you back!

Log Out

© 2024 NYCU DB HW3 112550151 周佳瑩. All rights reserved.

If the password is incorrect:



Login

Username:

Enter your username

Password:

Enter your password

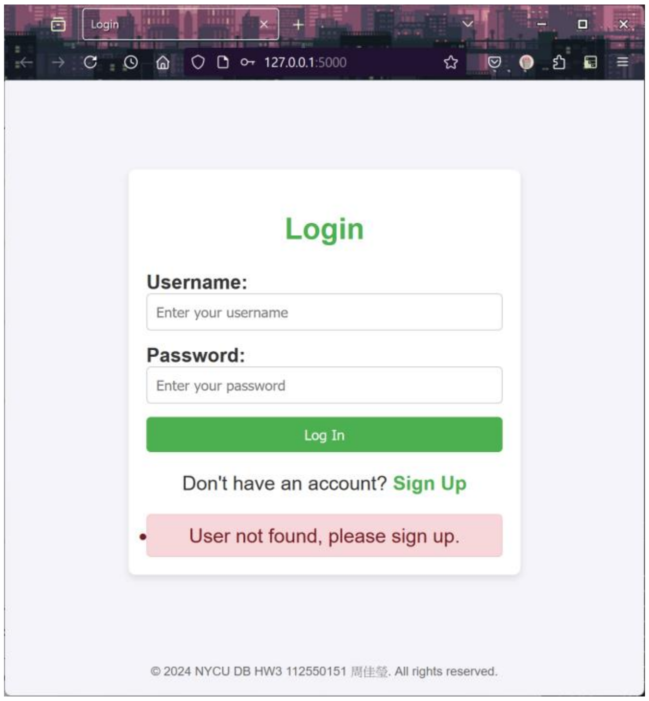
Log In

Don't have an account? Sign Up

- Password is incorrect.

© 2024 NYCU DB HW3 112550151 周佳瑩. All rights reserved.

If the user isn't in the database:



Login

Username:

Enter your username

Password:

Enter your password

Log In

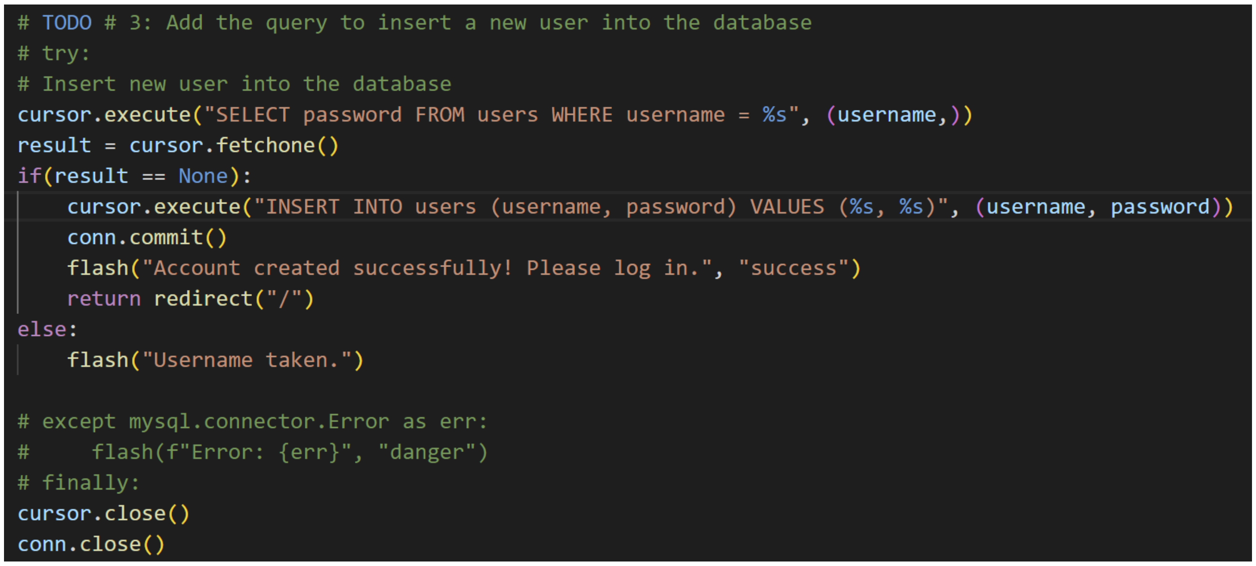
Don't have an account? Sign Up

- User not found, please sign up.

© 2024 NYCU DB HW3 112550151 周佳瑩. All rights reserved.

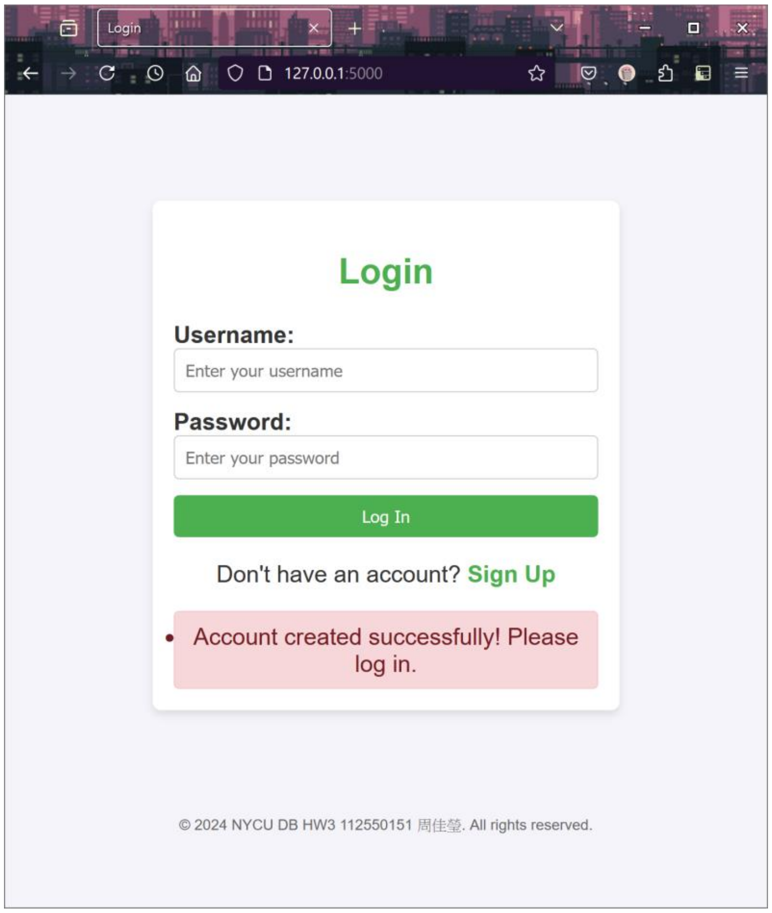
3. Screenshot and Explanation of Signup Function (5%)
   I used the cursor.execute from login to search for the username, if the username is taken, the website flashes "Username taken." and the user has to choose another username. If the username is available, the username and password are inserted into

the database and the user is redirected to the login page with the flash “Account created successfully! Please log in.”.



```
# TODO # 3: Add the query to insert a new user into the database
# try:
# Insert new user into the database
cursor.execute("SELECT password FROM users WHERE username = %s", (username,))
result = cursor.fetchone()
if(result == None):
    cursor.execute("INSERT INTO users (username, password) VALUES (%s, %s)", (username, password))
    conn.commit()
    flash("Account created successfully! Please log in.", "success")
    return redirect("/")
else:
    flash("Username taken.")

# except mysql.connector.Error as err:
#     flash(f"Error: {err}", "danger")
# finally:
cursor.close()
conn.close()
```

Created account successfully:



Login

Username:

Enter your username

Password:

Enter your password

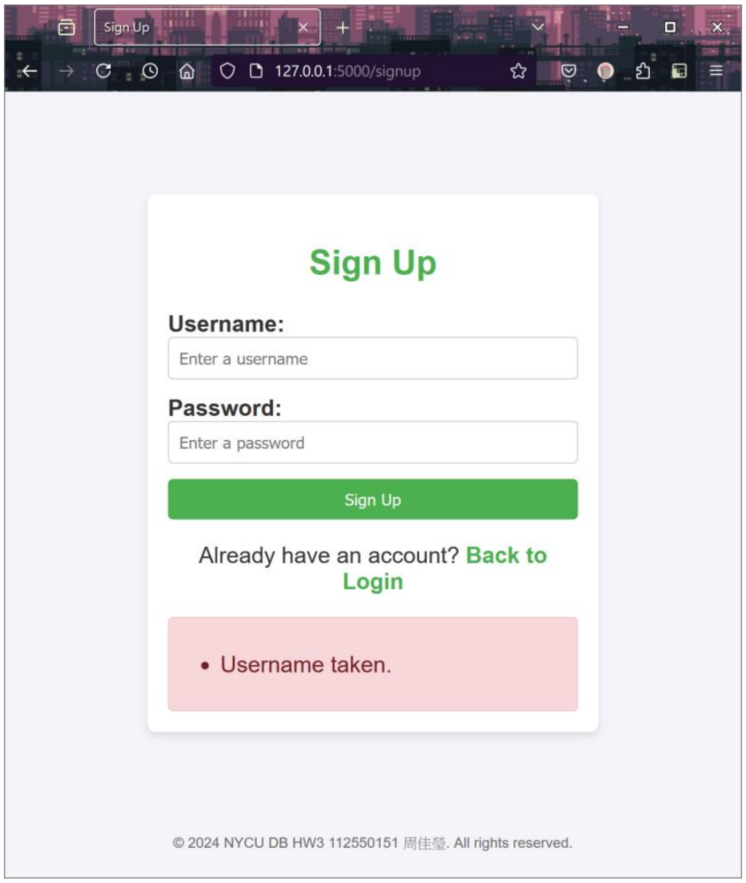
Log In

Don't have an account? Sign Up

- Account created successfully! Please log in.

© 2024 NYCU DB HW3 112550151 周佳瑩. All rights reserved.

Account not created:



Sign Up

Username:

Enter a username

Password:

Enter a password

Sign Up

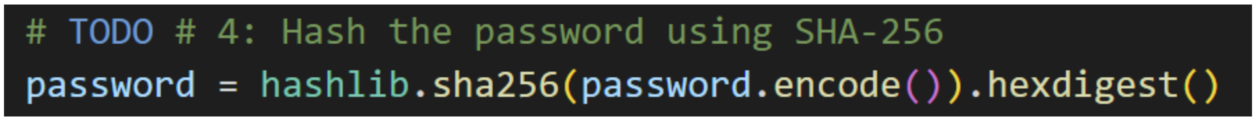
Already have an account? Back to Login

- Username taken.

© 2024 NYCU DB HW3 112550151 周佳瑩. All rights reserved.

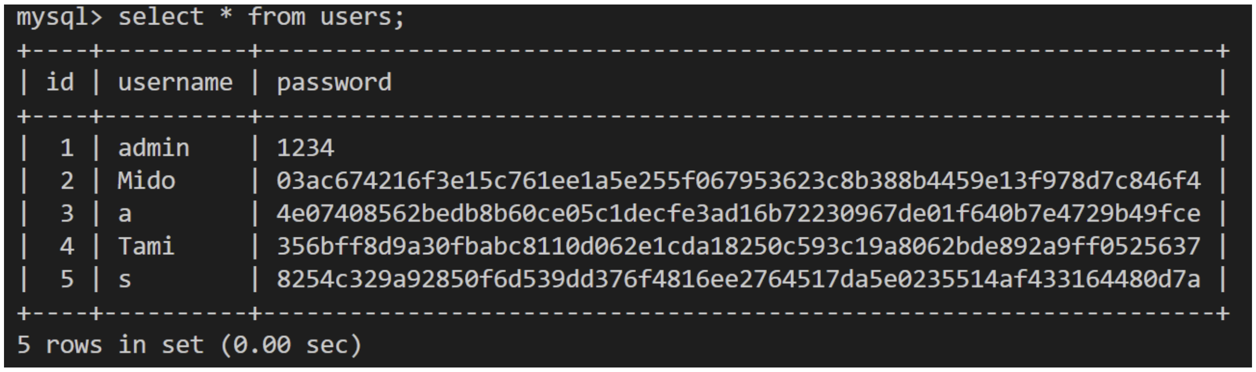
4. Screenshot of Hashed Passwords (5%)

   My password hashing code uses the function sha256 from the library hashlib. It first inputs the binary encoding of the password into sha256, then makes the hashed password hexadecimal.



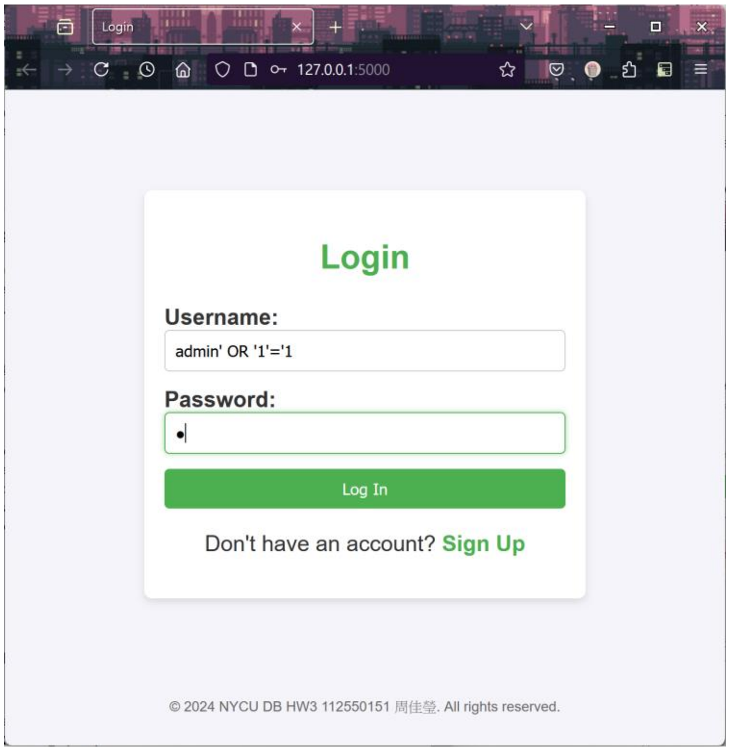
```
# TODO # 4: Hash the password using SHA-256
password = hashlib.sha256(password.encode()).hexdigest()
```

   Execution result of "SELECT * FROM users;" is shown in the screenshot below. The passwords are hashed.



```
mysql> select * from users;
+----+----------+------------------------------------------------------------------+
| id | username | password                                                         |
+----+----------+------------------------------------------------------------------+
|  1 | admin    | 1234                                                             |
|  2 | Mido     | 03ac674216f3e15c761ee1a5e255f067953623c8b388b4459e13f978d7c846f4 |
|  3 | a        | 4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b49fce |
|  4 | Tami     | 356bff8d9a30fbabc8110d062e1cda18250c593c19a8062bde892a9ff0525637 |
|  5 | s        | 8254c329a92850f6d539dd376f4816ee2764517da5e0235514af433164480d7a |
+----+----------+------------------------------------------------------------------+
5 rows in set (0.00 sec)
```

5. Screenshot and Explanation of SQL Injection Prevention (10%)
   Originally, the input of the username would directly be used in the SQL search query, which would result in the user being able to login because the query would provide results even if the username isn't in the database. I changed the code to "cursor.execute("SELECT password FROM users WHERE username = %s", (username,))" so the query wouldn't take the input directly but take a string in instead, so the input won't affect the query and yield fake results.
   The screenshots show what happens when the username is "admin' OR '1'='1".



Login

Username:

admin' OR '1'='1

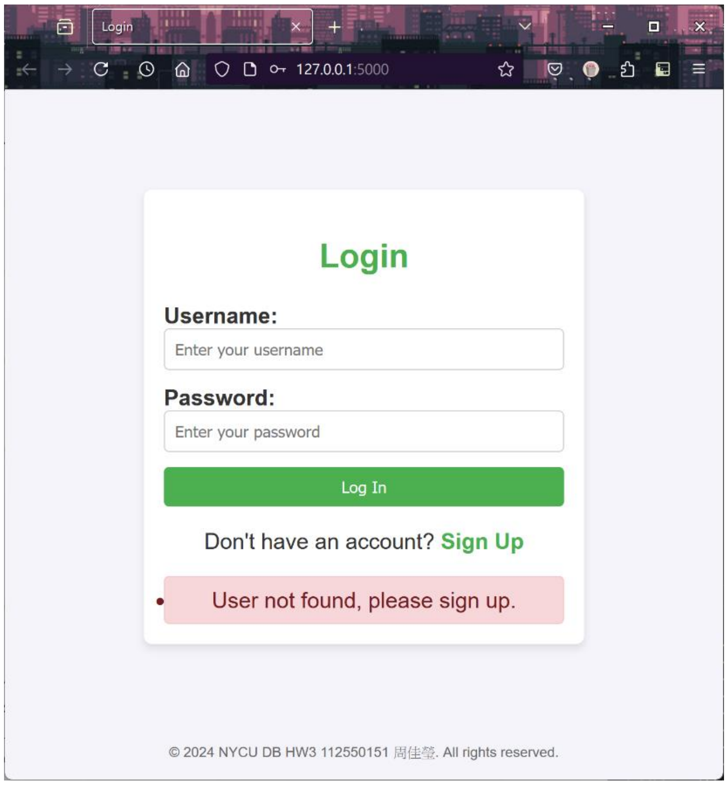
Password:

•

Log In

Don't have an account? Sign Up

© 2024 NYCU DB HW3 112550151 周佳瑩. All rights reserved.



Login

Username:

Enter your username

Password:

Enter your password

Log In

Don't have an account? Sign Up

User not found, please sign up.

© 2024 NYCU DB HW3 112550151 周佳瑩. All rights reserved.