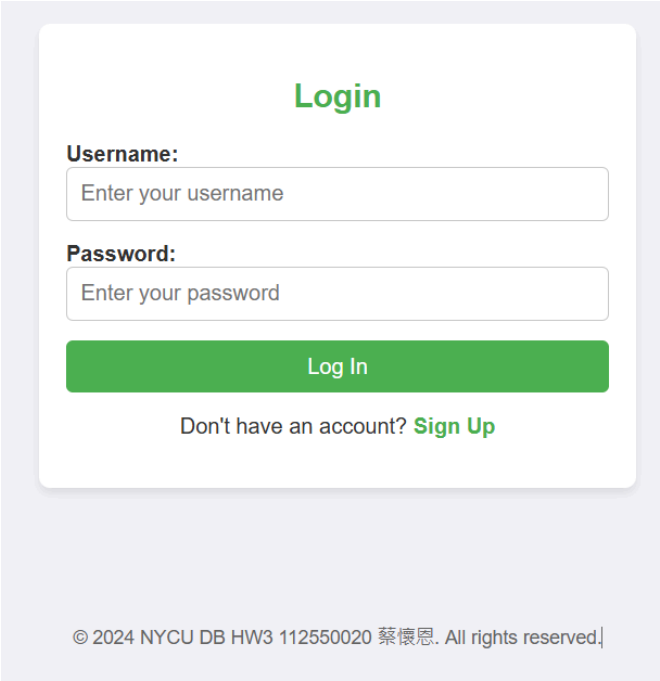
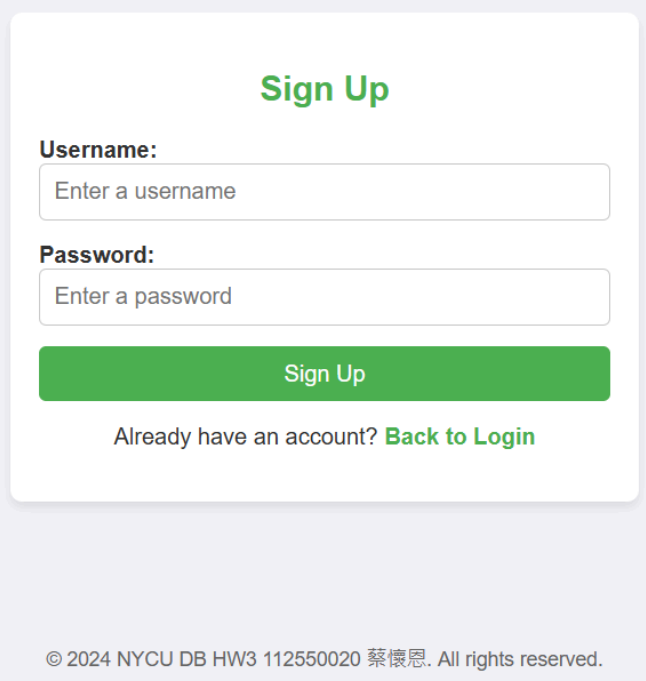
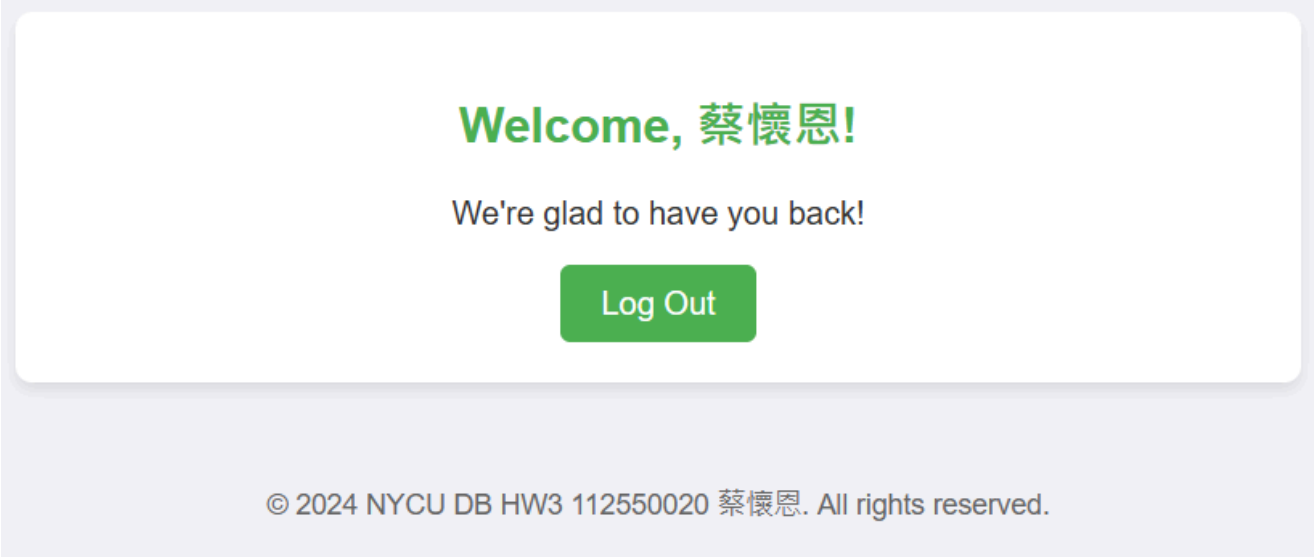
1. Footer

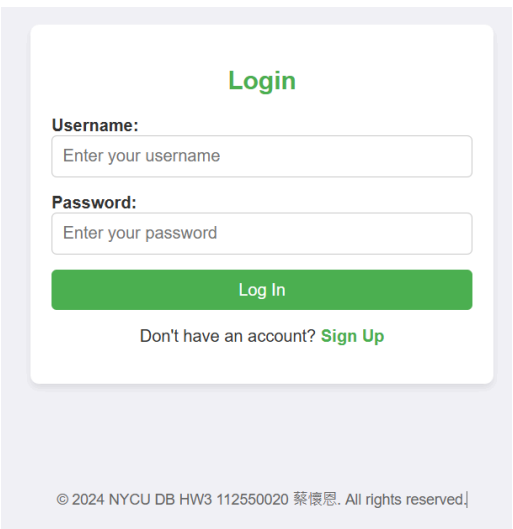

Login
Username:
Enter your username
Password:
Enter your password
Log In
Don't have an account? Sign Up
© 2024 NYCU DB HW3 112550020 蔡懷恩. All rights reserved.

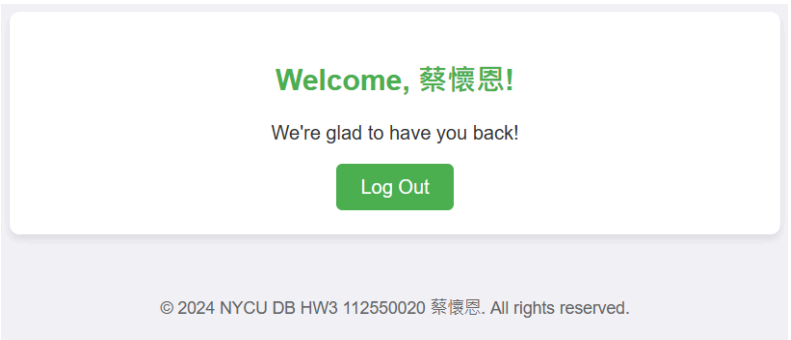

Sign Up
Username:
Enter a username
Password:
Enter a password
Sign Up
Already have an account? Back to Login
© 2024 NYCU DB HW3 112550020 蔡懷恩. All rights reserved.


Welcome, 蔡懷恩!
We're glad to have you back!
Log Out
© 2024 NYCU DB HW3 112550020 蔡懷恩. All rights reserved.

2. login

```python
# Login Page
@app.route("/", methods=["GET", "POST"])
def login():
    if request.method == "POST":
        username = request.form['username']
        password = request.form['password']

        # TODO # 4: Hash the password using SHA-256
        password = password.encode('utf-8')
        sha256 = hashlib.sha256()
        sha256.update(password)
        hash_value = sha256.hexdigest()


        # Connect to the database
        conn = get_db_connection()
        cursor = conn.cursor()

        # TODO # 2. Check if the user exists in the database and whether the password is correct
        # Query to check the user
        if username != "admin' OR '1'='1":
            cursor.execute(f"SELECT password FROM users WHERE username = '{username}'")
            result = cursor.fetchone() # fetchone() returns None if no record is found

        if username == "admin' OR '1'='1":
            flash("帳號或密碼錯誤","danger")
        elif result is None:
            flash("帳號或密碼錯誤","danger")
        elif result[0]==hash_value:
            session['username'] = username
            return redirect("/welcome")
        else:
            flash("帳號或密碼錯誤","danger")

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

    return render_template("login.html")
```

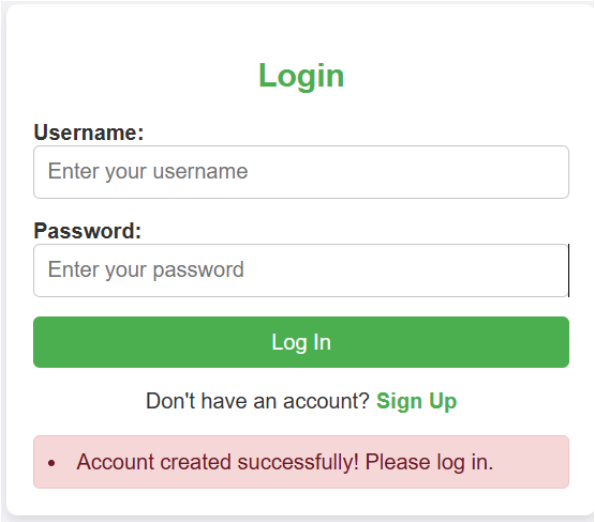


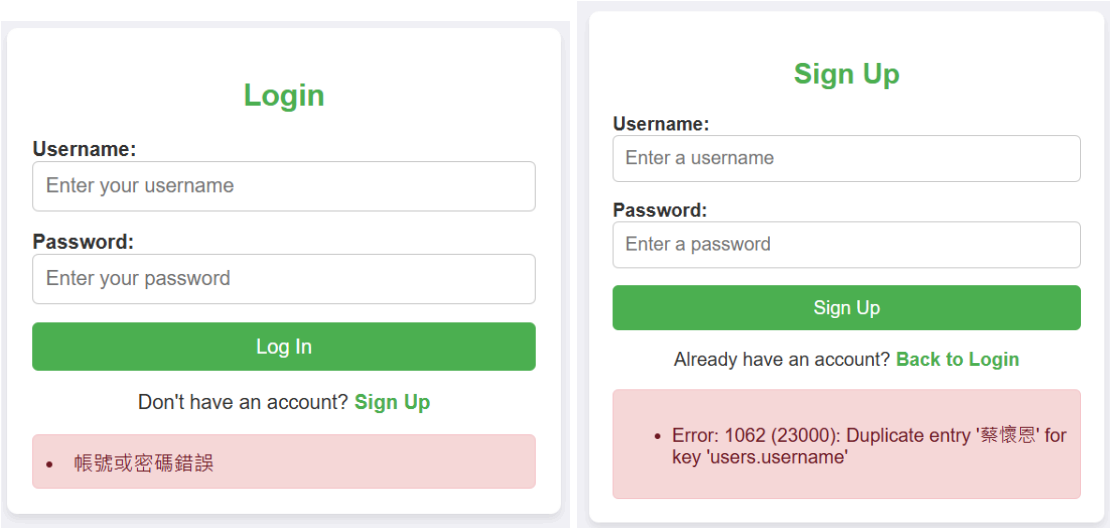


1.先輸入帳密
2.把密碼轉成SHA256
3.確認帳號不是admin' OR '1'='1 ,從database裡面找那組帳密
4.如果沒找到或是錯誤就顯示錯誤
5.正確就進到welcome

3.Signup

```python
# Signup
@app.route("/signup", methods=["GET", "POST"])
def signup():
    if request.method == "POST":
        username = request.form['username']
        password = request.form['password']

        # TODO # 4: Hash the password using SHA-256
        password = password.encode('utf-8')
        sha256 = hashlib.sha256()
        sha256.update(password)
        hash_value = sha256.hexdigest()

        # Connect to the database
        conn = get_db_connection()
        cursor = conn.cursor()

        # TODO # 3: Add the query to insert a new user into the database
        try:
            # Insert new user into the database
            cursor.execute(f" INSERT INTO users (username, password) VALUES ('{username}', '{hash_value}');")
            conn.commit()
            flash("Account created successfully! Please log in.", "success")
            return redirect("/")
        except mysql.connector.Error as err:
            flash(f"Error: {err}", "danger")
        finally:
            cursor.close()
            conn.close()

    return render_template("signup.html")
```





1.先輸入帳密
2.把密碼轉成SHA256
3.把帳號和SHA256的密碼insert到database
4.成功就回到login並顯示創建成功,請登入
5.錯誤就顯示錯誤

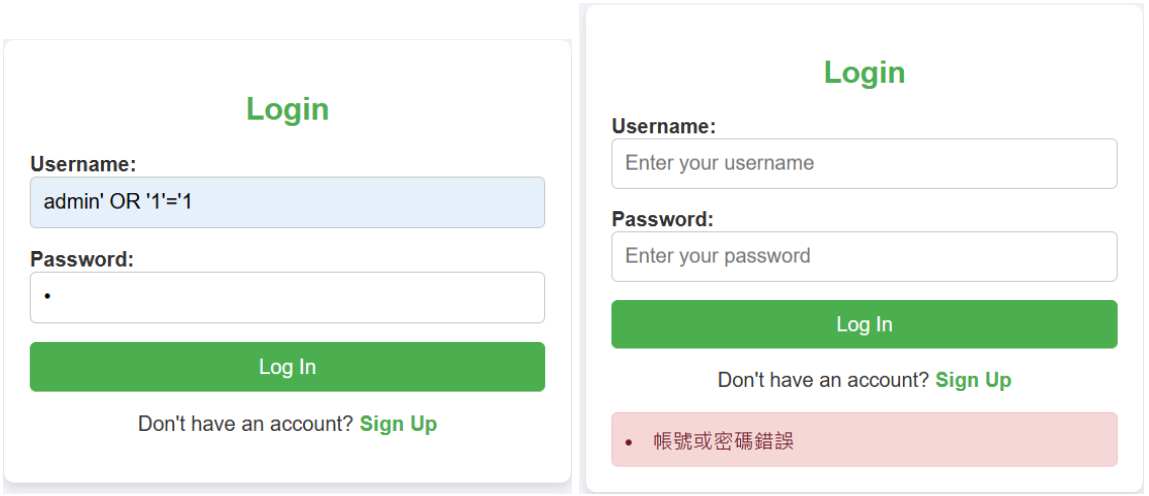
4.hash

```
import hashlib
```

```
# TODO # 4: Hash the password using SHA-256
password = password.encode('utf-8')
sha256 = hashlib.sha256()
sha256.update(password)
hash_value = sha256.hexdigest()
```

```
mysql> SELECT * FROM users;
+----+-----------+------------------------------------------------------------------+
| id | username  | password                                                         |
+----+-----------+------------------------------------------------------------------+
|  8 | wayne     | a982c97d452cc71fde02409d6e6a623220c882930c3c13ab7733e61bc9870b6c |
|  9 | 蔡懷恩    | 2208ddabfee915957ee09836cae0c2298faf6413d77192dd79d192cda59590b6 |
| 11 | admin     | 03ac674216f3e15c761ee1a5e255f067953623c8b388b4459e13f978d7c846f4 |
+----+-----------+------------------------------------------------------------------+
3 rows in set (0.00 sec)
```

5.Injection Prevention




```python
if username != "admin' OR '1'='1":
    cursor.execute(f"SELECT password FROM users WHERE username = '{username}'")
    result = cursor.fetchone() # fetchone() returns None if no record is found

if username == "admin' OR '1'='1":
    flash("帳號或密碼錯誤","danger")
elif result is None:
    flash("帳號或密碼錯誤","danger")
elif result[0]==hash_value:
    session['username'] = username
    return redirect("/welcome")
else:
    flash("帳號或密碼錯誤","danger")
```

方法:跑進sql前，直接檢查輸入的username，如果是admin' OR '1'='1就直接顯示錯誤