Jake Christianson

1. Why is password hashing important in secure applications?
    a. It protects users' passwords even if the database is compromised as it converts plain text passwords into fixed length, and it is an irreversible string. This makes it very difficult for hackers to recover original passwords.
2. What would be the risk if passwords were stored in plain text?
    a. If the database is compromised all the user passwords are immediately leaked. And because users reuse passwords so other accounts there entire internet passwords are at risk.
3. What is the role of BCryptPasswordEncoder?
    a. It provides strong one way password hashing using the BCrypt algorithm, as it prevents rainbow table attacks. This makes the brute force attack a lot slower due to its adjustable computational cost.
4. How does your app check for and prevent duplicate users?
    a. It checks the database for an existing username or email before creating a new user, while also rejecting registration if a duplicate is found.

Description: Register a new user with a unique username and secure password.

Try it out!

Username:

Jake7

Password:

•••••

Register User

```
201 : User registered successfully
```

POST `/login`

Description: Authenticate an existing user with username and password verification.

Try it out!

Username:

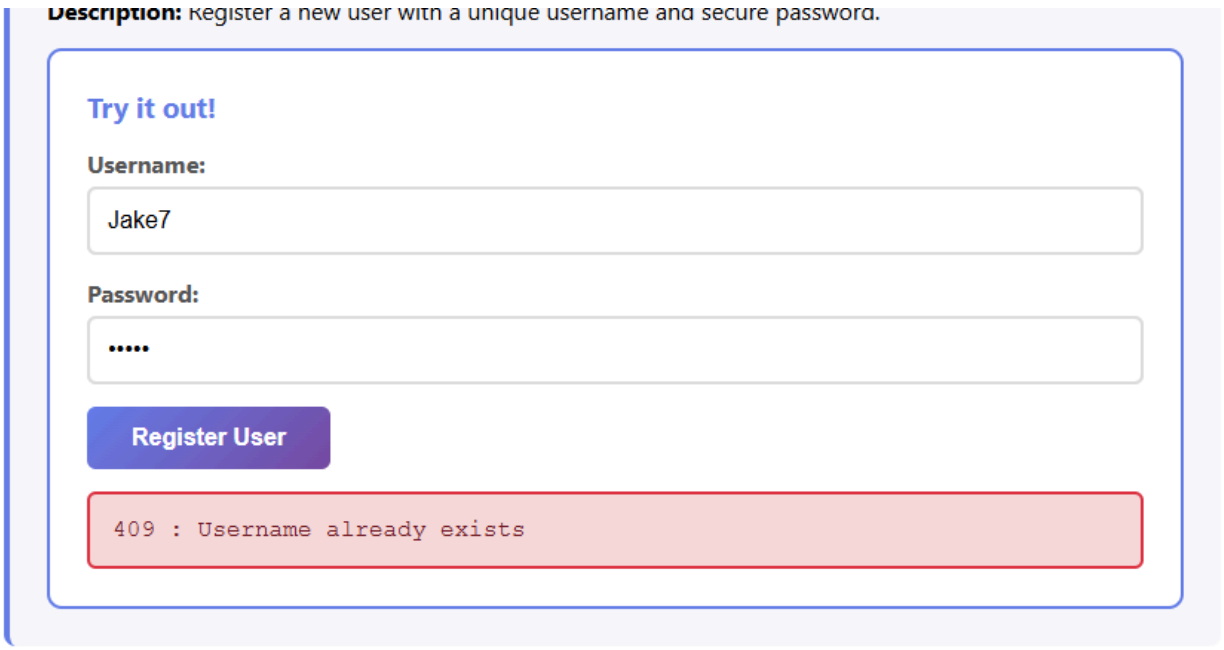
Jake

Password:

•••••

Login

```
401 : Invalid username or password
```



Description: Register a new user with a unique username and secure password.

Try it out!

Username:

Jake7

Password:

•••••

Register User

```
201 : User registered successfully
```

POST `/login`

Description: Authenticate an existing user with username and password verification.

Try it out!

Username:

Jake7

Password:

•••••

Login

```
200 : Login successful
```