User Registration:

- Encrypt passwords: Use bcrypt to hash passwords before storing them in the database.
- Ensure strong password with some rules (minimum length, mixed characters, etc).
- Validate that each user has a unique email and username.

Login:

- Secure login: Implement a login flow where the user inputs their email/username and password then check the hashed password against the stored version.
- Token-based authentication: Generate JSON web token upon successful login, which is sent back to the user and stored in their browser.
- Use tokens to authenticate requests for protected resources.

Password Recovery:

- Provide a password reset functionality by sending a one-time link to the user's email. This link should expire after a set time.
- Use secure random tokens in the recovery email.

Tools and Frameworks:

- Passport.js: A popular Node.js library for handling authentication strategies, such as JSON web tokens or OAuth.
- bcrypt.js: For hashing and verifying user passwords.
- jsonwebtoken: For creating and verifying JWT tokens.
- Nodemailer: For sending password recovery emails.