

**Digital Newspaper Website
Use-Case Specification: Login**

Version 1.0

404 Not Found

Revision History

Date	Version	Description	Author
16/07/2025	1.0	Specific about Login use case	Nguyễn Tấn Lộc

Table of Contents

1. Use-Case Name: Login	4
1.1 Brief Description	4
2. Flow of Events	4
2.1 Basic Flow	4
2.2 Alternative Flows	4
2.2.1 Invalid Credentials	4
2.2.2 Account Locked	4
3. Special Requirements	4
3.1 Security	4
3.2 Session management	4
3.3 Responsiveness	5
3.4 Accessibility	5
4. Preconditions	5
4.1 The user must already have a registered account in the system	5
4.2 The system is online and accessible	5
5. Postconditions	5
5.1 The user is authenticated and session is started	5
5.2 The user gains access to restricted content and user-specific features	5
5.3 The login attempt is logged (for auditing and security tracking)	5

Use-Case Specification: Login

1. Use-Case Name: Login

1.1 Brief Description

This use case describes how a registered user accesses their account by providing a valid username and password. If the credentials are correct, the system grants access and sets the session, if not, an error message is shown. Users may also request password recovery if needed.

2. Flow of Events

2.1 Basic Flow

1. The user click the login button from the homepage
2. The system displays the login form with fields: email/ username and password
3. The user enter their credentials and clicks submit button
4. The system validates the inputs:
 - a. Check mail/ username is existed
 - b. Verifies password
5. If the credentials are correct
 - a. The system authenticates the user
 - b. Sets a session token or login cookie
 - c. The system displays the homepage with user` personal account
6. The user is now logged in and can access authenticated features

2.2 Alternative Flows

2.2.1 *Invalid Credentials*

- In step 4, credential do not matching

2.2.1.1 An Alternative Subflow

- The system displays an error message “Invalid email or password. Please try again.”.
- Allow all users to re-enter credentials or choose password recovery

2.2.2 *Account Locked*

- The user enters incorrect credentials to much (e.g 5 times)

2.2.2.1 An Alternative Subflow

1. The system locks the account temporarily (e.g 5 minutes)
2. Display message “ your account is temporarily locked due to many failed login attempts”

3. Special Requirements

3.1 Security

- Passwords must be kept confidential to avoid information leakage.

3.2 Session management

- Session tokens or cookies must expire after a predefined period (eg. 1 hour)

404 Not Found

3.3 Responsiveness

- The login must render properly on all screen sizes

3.4 Accessibility

- The form must comply with WCAG 2.1 for screen readers and keyboard navigation

4. Preconditions

4.1 The user must already have a registered account in the system

4.2 The system is online and accessible

5. Postconditions

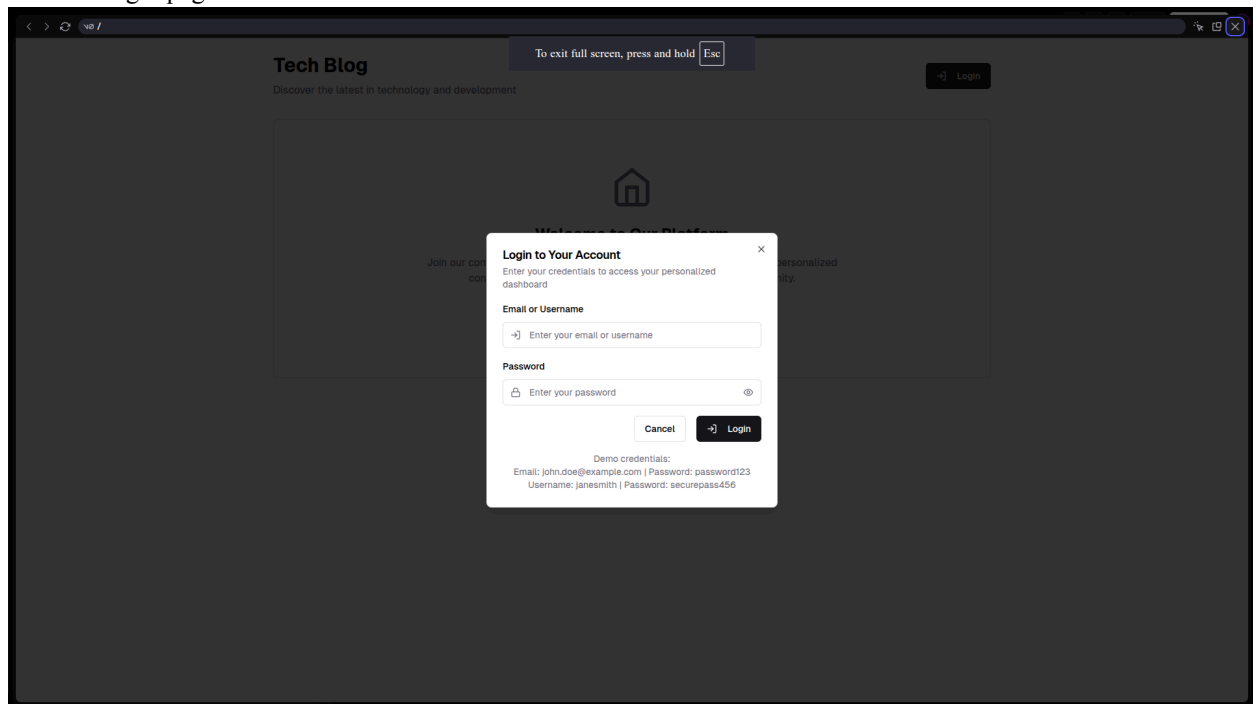
5.1 The user is authenticated and session is started

5.2 The user gains access to restricted content and user-specific features

5.3 The login attempt is logged (for auditing and security tracking)

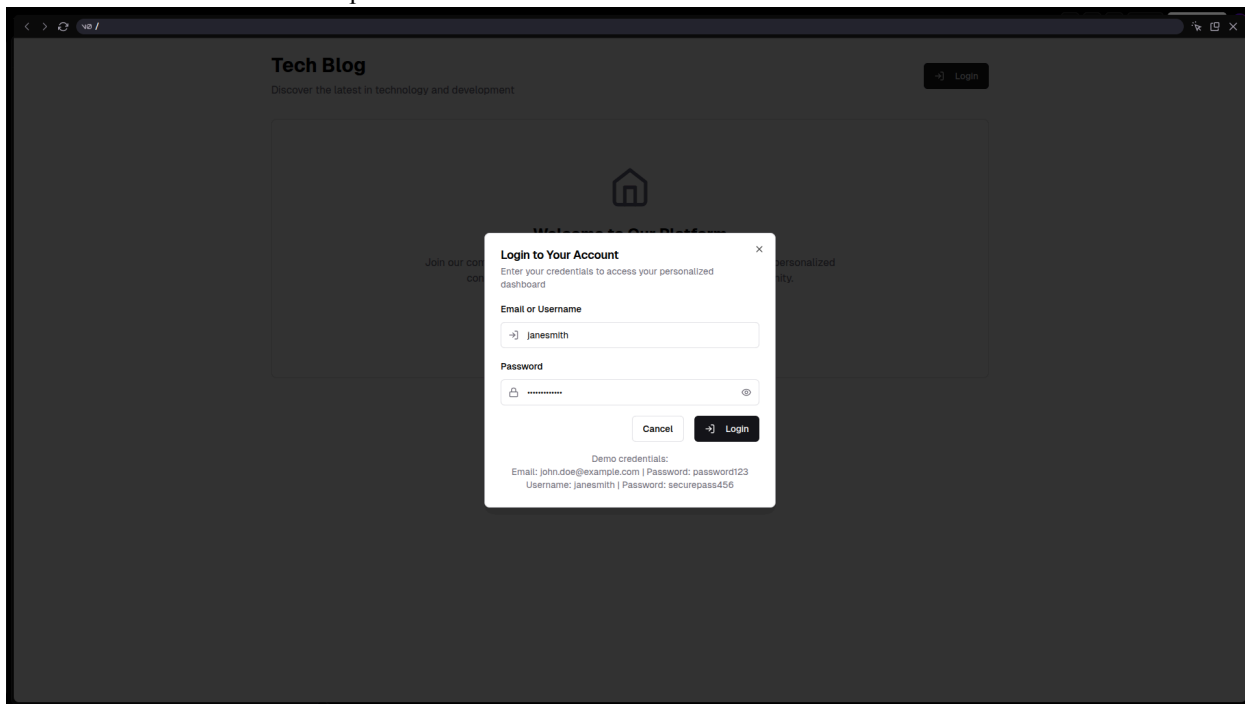
6. Generate Interface

Interface login page



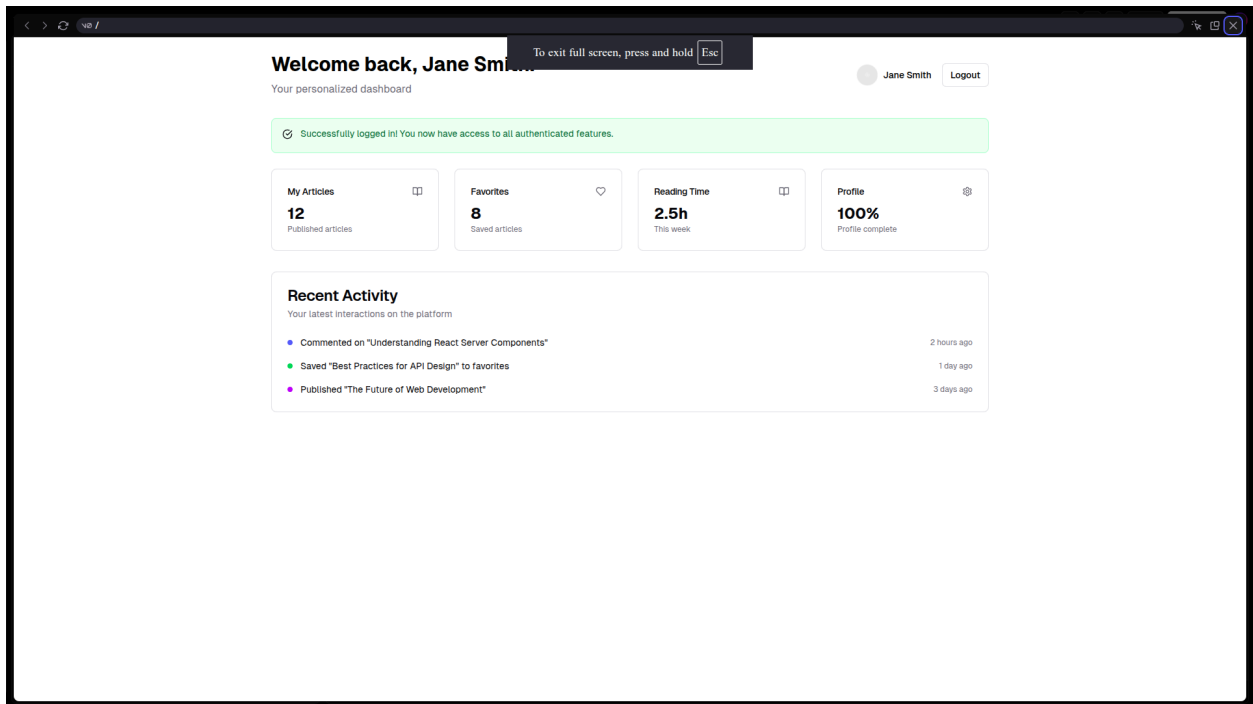
404 Not Found

User enter credentials username password

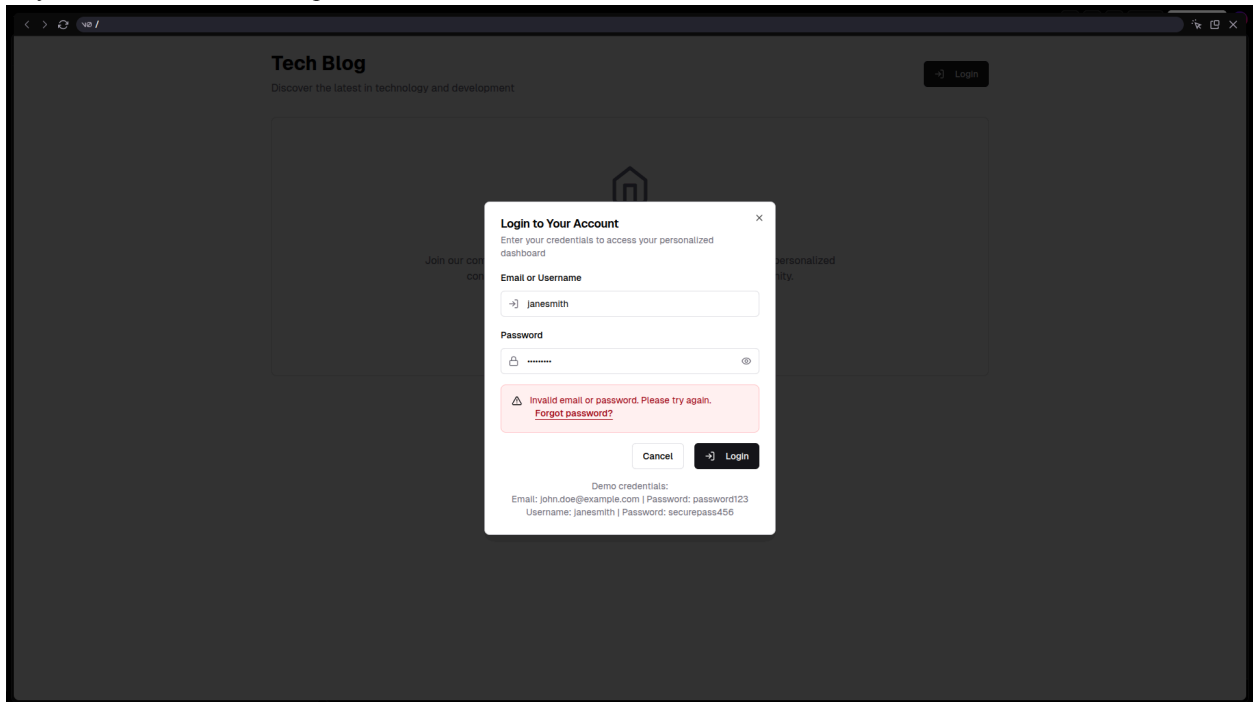


The system display screen when logged in successfully

404 Not Found



If system check username or password are false



404 Not Found
