Book Alley

Use-Case Specification: Login

Version 1.0

Revision History

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
| 09/11/2023 | 1.0 | Initial | Dang Ha Huy |
| 17/11/2023 | 2.0 | Review | Phung Sieu Dat |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[**1. Use-Case Name 4**](#_heading=h.30j0zll)

[1.1 Brief Description 4](#_heading=h.1fob9te)

[**2. Flow of Events 4**](#_heading=h.3znysh7)

[2.1 Basic Flow 4](#_heading=h.2et92p0)

[2.2 Alternative Flows 4](#_heading=h.tyjcwt)

[2.2.1 Invalid credentials 4](#_heading=h.3dy6vkm)

[2.2.2 Account lockout 4](#_heading=h.uw6tausdrp5n)

[2.2.3 Two-factor authentication 4](#_heading=h.uyxegjw2emz)

[**3. Special Requirements 5**](#_heading=h.4d34og8)

[3.1 Security 5](#_heading=h.2s8eyo1)

[3.2 User experience 5](#_heading=h.w5h01a98mda8)

[3.3 Performance 5](#_heading=h.zcc52lmbsk9d)

[3.4 Compatibility 5](#_heading=h.2xtpsiuct0xk)

[**4. Preconditions 5**](#_heading=h.17dp8vu)

[4.1 Internet connectivity 5](#_heading=h.3rdcrjn)

[4.2 User account exists 5](#_heading=h.ao59k2qmmp1)

[4.3 Website is accessible 5](#_heading=h.xvq0kx73sbci)

[4.4 Compatibility 5](#_heading=h.uoymipe8ruf0)

[4.5 Account not locked 5](#_heading=h.ru94aym8da72)

[**5. Postconditions 6**](#_heading=h.26in1rg)

[5.1 Login successfully 6](#_heading=h.lnxbz9)

[5.2 Session Management 6](#_heading=h.tuvijemqy6eu)

[5.3 Account lockout 6](#_heading=h.bqy3ll8rw923)

[5.4 Error Handling 6](#_heading=h.oba5tqanfxp5)

[5.5 Logging in and security 6](#_heading=h.d1rkx7pmklvd)

[**6. Extension Points 6**](#_heading=h.35nkun2)

[6.1 Forgotten password 6](#_heading=h.t30n155680m)

[6.2 Captcha 6](#_heading=h.dhmxlpxuiv23)

[6.3 Two-step verification 6](#_heading=h.khw4onywz07e)

[6.4 Social media login 6](#_heading=h.9mu7ettticfv)

Use-Case Specification: Login

# Use-Case Name

## Brief Description

The login use case of Book Alley allows users with an account to securely login to their account and enables them to use other functions of the web application.

# Flow of Events

## Basic Flow

1. The user access the website through an internet browser
2. The user is first met with a homepage, they can choose the account icon on the top right to login
3. The website presents to them the login screen
4. The user enters valid credentials then the system grants them access to their account and redirects them to the homepage
5. A session is created to maintain the user's login state, allowing them to access their account's features without repeated logins.
6. The user can now use the website's features and access their personalized content.

## Alternative Flows

### Invalid credentials

1. The user navigates to the login page
2. The user enters invalid credentials
3. The system detects that the credentials are invalid and displays an error message to the user, prompting them to re-enter their credentials
4. The user attempt to login again
5. The system continues to validate and the user repeats the login process until the credentials are valid or the user abandons the login process

### Account lockout

1. The user navigates to the login page
2. The user enters invalid credentials multiple times
3. After a predefined number of failed login attempts, the system locks the user's account to prevent further unauthorized access.
4. The system displays an account lockout message, informing the user that their account has been temporarily locked.
5. The user can initiate an account recovery process, such as resetting their password or contacting customer support.

### Two-factor authentication

1. The user navigates to the login page
2. The user enters their credentials
3. The system checks the entered credentials against the stored user account information in the database.
4. If the credentials are valid, the system prompts the user for a second authentication factor
5. The user enters the 2FA code.
6. The system validates the code. If it's correct, the user gains access to their account; otherwise, they are prompted to retry.

# Special Requirements

## Security

* The login process must be secure, using strong encryption protocols to protect the user’s information.
* Passwords should be securely stored using encryption techniques, such as hashing and salting.
* Implement measures to prevent brute-force attacks, such as account lockouts after a certain number of failed login attempts.
* Implement mechanisms to detect and prevent account hijacking, such as detecting suspicious login patterns or IP addresses.

## User experience

* The login page must be intuitive, provide clear instructions and easy to use even for non-technical users
* The login page must also provide the user with other essential functions such as a register function to enable users to create a new account and a password recovery function for users who have forgotten their credentials.
* Provide a "Remember Me" checkbox option on the login page to allow users to stay logged in across multiple sessions or after closing their browser.

## Performance

* The login process must be fast, responsive, the delay must be under 5 seconds
* The login functionality should be able to handle a large number of concurrent login requests without significant performance degradation.
* Cache frequently accessed data, such as user credentials or session information, to reduce database queries and improve performance.

## Compatibility

* Login functionality must be supported on many popular browser such as Chrome, Edge, Firefox, Opera, etc
* Ensure that the login page and associated elements are responsive and mobile-friendly.
* Support multiple languages and character sets to cater to a diverse user base.

# Preconditions

## Internet connectivity

* The user’s PC must have an internet connection to access the website and communicate with the website’s servers for authentication and other functions.

## User account exists

* Before a user can log in, there must be an existing user account for them in the system. This means the system must have stored the user's credentials and profile information.

## Website is accessible

* The website must be up and running, and the user must have access to it. If the website is down or inaccessible, the login cannot occur.

## Compatibility

* The customer's device (computer, smartphone, tablet) should meet the compatibility requirements of Book Alley web application.

## Account not locked

* The user's account should not be locked or suspended due to multiple unsuccessful login attempts or any other reason.

# Postconditions

## Login successfully

* If the user provided valid credentials then the website authenticates them and leads the user to the homepage.

## Session Management

* The system generates a unique session identifier or token for the customer's session after successful login.
* The session identifier is associated with the customer's account and used for subsequent requests to maintain the authenticated state.

## Account lockout

* If the login process encounters multiple failed login attempts or suspicious activity, the system may enforce an account lockout mechanism.
* In such cases, the customer's account may be temporarily locked or restricted from further login attempts for a specified duration to enhance security.

## Error Handling

* If the login process encounters any errors or exceptions, appropriate error messages are displayed to the user, indicating the nature of the issue.

## Logging in and security

* Appropriate logging and security measures should be in place to track and protect the user's login information and the system's data. This might include measures like password encryption and secure communication.

# Extension Points

## Forgotten password

* This extension point can be triggered when a user has forgotten their password and needs to reset it. The use case can be extended to include a "Password Reset" feature, allowing the user to regain access to their account.

## Captcha

* This extension point can be triggered when there is a need for additional security measures to prevent automated or brute-force login attempts. It can be extended to include the use of CAPTCHA verification or other security challenges.

## Two-step verification

* In scenarios where a user has enabled two-step verification for their account, this extension point can be triggered to accommodate the additional step in the login process.

## Social media login

* If the system supports social media login, this extension point can be triggered, allowing users to log in using their social media accounts such as Google, Facebook, Twitter, etc.