Book Alley

Use-Case Specification: Registration

Version 1.0

Revision History

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
| 09/11/2023 | 1.0 | Initial | Dang Ha Huy |
| 17/11/2023 | 2.0 | Update Special Requirements, Preconditions and Postconditions | Tran Minh Hai Uyen |
|  |  |  |  |
|  |  |  |  |

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 data 4](#_heading=h.3dy6vkm)

[2.2.2 Password strength 4](#_heading=h.1t3h5sf)

[2.2.3 If user already have an account 4](#_heading=h.lka2uov0a3tn)

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

[3.1 Security 4](#_heading=h.2s8eyo1)

[3.2 User experience 4](#_heading=h.w5h01a98mda8)

[3.3 Performance 4](#_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 access 5](#_heading=h.5hl05lmkmk0i)

[4.3 User information 5](#_heading=h.mmfvene2fq7m)

[4.4 No duplicate account 5](#_heading=h.dfau774e9zgp)

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

[5.1 Account created 5](#_heading=h.lnxbz9)

[5.2 User login 5](#_heading=h.tuvijemqy6eu)

[5.3 User credentials 5](#_heading=h.bqy3ll8rw923)

[5.4 Access to user profile 5](#_heading=h.vs69zr2uq5el)

[5.5 Error handling 5](#_heading=h.cck0mpihws0q)

[**6. Extension Points 5**](#_heading=h.35nkun2)

[6.1 Social media integration 5](#_heading=h.1ksv4uv)

[6.2 Two-factor authentication 5](#_heading=h.8yby1xzh1l53)

[6.3 Multi-language support 5](#_heading=h.xunbv6dszijo)

[6.4 Captcha 6](#_heading=h.txhxw9y14e2)

[6.5 Third-party integration 6](#_heading=h.c2rpjz1hp3f6)

[6.6 User notification 6](#_heading=h.rn7thfqkvnw9)

Use-Case Specification: Registration

# Use-Case Name

## Brief Description

The registration use case for Book Alley enables user to create a new account to gain access to the all of the website features

# Flow of Events

## Basic Flow

1. The user navigates to the register page when click on “Register now” on the login page
2. The user is presented with a registration form to enter their information such as username, email, password
3. The user click “Submit” to submit the registration form
4. The system checks for valid data, ensuring that the email address is in the correct format, the username is not already in use, and the password meets security requirements.
5. If the data is valid, the system creates a new user account and stores the user's information in the database.
6. The system displays a confirmation message, indicating that the registration was successful.
7. The user is now able to log in using the newly created account.

## Alternative Flows

### Invalid data

1. If the system detects invalid data (e.g a poorly formatted email address or an already existing username), the user is prompted to correct the errors
2. The user then re-enter their information

### Password strength

1. If the user's chosen password does not meet the required security criteria (e.g., minimum length, including numbers and special characters), they are prompted to choose a stronger password
2. The user then re-enter their password to comply with the restriction

### If user already have an account

1. If the system detects the email that the user use to register already link to an account then they are notify with a message indicate that the email have been registered
2. The user is redirected back to the login screen

# Special Requirements

## Security

* The registration process must adhere to industry-standard security practices to protect user information and prevent unauthorized access. This includes using strong encryption protocols to safeguard data transmission between the user's device and the server.
* User passwords must be hashed using secure and industry-standard algorithms, to store them in a non-reversible format. This prevents the exposure of plaintext passwords in the event of a data breach.
* The registration system should implement measures to prevent common security vulnerabilities, which could be exploited to compromise user accounts or gain unauthorized access to the system.

## User experience

* The registration page should be designed with a user-centered approach, ensuring that it is intuitive, easy to navigate, and accessible to users of all technical backgrounds.
* The registration form should be optimized for simplicity and efficiency, minimizing the number of required fields and avoiding unnecessary complexity.
* The registration process should provide feedback mechanisms to inform users of any errors or omissions in their input.

## Performance

* The registration process must be designed for efficiency and responsiveness, ensuring that it can handle user requests quickly and without delays.
* The registration page should be optimized for page load speed, ensuring that it loads quickly and seamlessly for users with varying internet connections.
* The registration process should be able to handle a high volume of concurrent user requests without performance degradation.

## Compatibility

* The registration page should be compatible with major web browsers, including Chrome, Firefox, Safari, and Edge, to ensure accessibility across a wide range of devices and operating systems.
* The registration page should be responsive and adapt seamlessly to different screen sizes and resolutions, ensuring a consistent user experience across desktops, laptops, tablets, and mobile devices.

## Server Functionality:

* The server infrastructure supporting the registration process must be robust, scalable, and highly available to handle user requests reliably and efficiently.
* The server software should be properly configured and updated to the latest versions to ensure optimal performance, security, and compatibility.
* The server environment should be monitored and managed effectively to identify and resolve any performance bottlenecks or potential issues before they impact user experience.

# Preconditions

## Internet connectivity

* The user's device must have a stable internet connection with sufficient bandwidth to access the registration page and submit the data promptly. Intermittent or slow internet connectivity can lead to delays, errors, or an inability to complete the registration process.

## User access

* The website should be accessible to the user, and they should be able to navigate to the registration page without encountering any technical or accessibility issues. This includes ensuring that the website is compatible with the user's device and browser and that there are no redirects or other obstacles preventing access.

## User information

* The user should have the necessary information required for registration readily available. This includes a valid email address that can receive confirmation emails, a unique username that complies with the website's guidelines, and a strong password that meets complexity requirements.

## No duplicate account

* The user should not already have an account with the same email address or username. If the system does not allow duplicate accounts, the registration process should check for existing accounts and prevent the user from creating a new one using the same credentials.

## Unique Identity

* Users should not be allowed to create multiple accounts using the same identifying information. This prevents users from circumventing registration restrictions or creating multiple accounts for malicious purposes.

## Required Fields

* All mandatory fields on the registration page, such as email address, password, and username, should be clearly identified and marked. This helps the user understand the information required to complete the registration process and avoid leaving essential fields blank.

## Data Format

* Input fields for user information should have appropriate data format restrictions to prevent invalid entries. For example, the email address field should only accept valid email formats, the password field should enforce complexity requirements, and other fields should accept data in the expected format.

## Data Uniqueness

* The registration system should check if the email address or username provided by the user is already associated with an existing account. If so, the system should prevent the user from creating a new account using those credentials and prompt them to try a different email address or username.

## Error Messages

* Clear and informative error messages should be displayed when users enter invalid or missing information. This helps the user identify and correct any errors in their input to ensure successful registration.

## Password Confirmation

* Users should be prompted to confirm their password by entering it twice. This helps ensure that the password is entered correctly and prevents typos or misspellings that could lead to login difficulties later.

# Postconditions

## Account creation

* Upon successful registration, the platform should create a new account for the user in the system's database. The newly created account should be seamlessly integrated with the platform's user authentication system, ensuring that the user can log in using their credentials and access the platform's features.

## Account activation:

* The user's account should be activated immediately upon registration, allowing them to access the platform's features. The account activation process should be transparent and user-friendly.

## Account verification:

* If applicable, the platform should initiate an account verification process, such as email or mobile phone verification, to ensure user authenticity. This additional layer of security safeguards the platform from spam, malicious activities, and unauthorized access to user accounts.

## User credentials

* The system should provide the user with information on how to log in, typically with their new username and password. The user credentials should be handled securely and in accordance with data privacy regulations. The password should be stored in a hashed format to prevent plaintext disclosure, and appropriate measures should be in place to protect against unauthorized access or retrieval of user credentials.

## Access to user profile

* Upon registration, the user should be able to access and customize their profile. This includes viewing their personal information, managing their preferences, and updating their profile details. The user profile should serve as a centralized hub for managing their account settings and personal information.

## Error handling

* In the event of a registration failure (e.g., due to a duplicate email or username), appropriate error messages should be displayed to the user, guiding them on how to resolve the issue.communication. Error messages should be formulated in a clear, concise, and informative manner, avoiding technical jargon or overly complex explanations.

# Extension Points

## Social media integration

* Allowing users to create or log into their accounts using their existing social media profiles, such as Facebook, Google, or Twitter. This eliminates the need for users to create and remember additional passwords, and it can also help to increase user engagement by making it easier for them to connect with their friends and followers on the website.

## Two-factor authentication

* Two-factor authentication (2FA) adds an extra layer of security to the registration process by requiring users to verify their identity using a second factor, in addition to their password. This could be a code sent to their phone via SMS or email, or a fingerprint scan. 2FA can help to protect user accounts from unauthorized access, even if their password is compromised.

## Multi-language support

* Enable the website to be displayed in multiple languages, making it accessible to a wider audience. Users can choose their preferred language during registration, and the website will automatically adjust its content accordingly. This can help to improve the user experience for non-native speakers.

## Captcha

* During registration, users will be presented with a captcha, which could be a visual puzzle or a text-based question. If the user can correctly answer the captcha, they will be allowed to proceed with registration. Captchas can help to prevent automated registration by bots, which can create fake accounts and spam the website.

## Third-party integration

* Allowing the website to integrate with third-party services, such as payment gateways or loyalty programs. For example, a website that sells products could integrate with a payment gateway to process credit card payments during registration. Or, a website that offers a loyalty program could integrate with the program to allow users to earn rewards during registration.

## User notification

* Allowing the website to send notifications or prompts to users during registration about helpful features, tips, or opportunities to complete their profiles. For example, the website could notify users about the benefits of creating a complete profile, or it could prompt them to subscribe to a newsletter. User notifications can help to improve the user experience and encourage users to engage more actively with the website.