Book Alley

Use-Case Specification: Forgot Password

Version 2.0

Revision History

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
| 11/11/2023 | 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=)

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

[2.2.2 Expired or invalid reset link 4](#_heading=h.1t3h5sf)

[2.2.3 Account lockout 4](#_heading=h.3c46gjw5w843)

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

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

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

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

[3.4 Regular backup 5](#_heading=h.yicw3wmyb1ux)

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

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

[4.2 User is registered 5](#_heading=h.5hl05lmkmk0i)

[4.3 Valid email address 5](#_heading=h.mmfvene2fq7m)

[4.4 System availability 5](#_heading=h.dfau774e9zgp)

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

[5.1 Password reset successful 5](#_heading=h.lnxbz9)

[5.2 Notification sent 5](#_heading=h.tuvijemqy6eu)

[5.3 Expired link 5](#_heading=h.bqy3ll8rw923)

[5.4 User feedback 5](#_heading=h.vs69zr2uq5el)

[5.5 Security audit 5](#_heading=h.cck0mpihws0q)

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

[6.1 Custom email templates 5](#_heading=h.1ksv4uv)

[6.2 Integration with external identity providers 6](#_heading=h.8yby1xzh1l53)

[6.3 Integration with Password Management Tools 6](#_heading=h.2qh1hz1nre8v)

[6.4 Two-Factor Authentication (2FA) 6](#_heading=h.rh1glr9n0044)

[6.5 Multi-Channel Password Reset 6](#_heading=h.inefdubxt2mi)

[6.6 Logging and analytics hooks 6](#_heading=h.5xtw6lnhnuy5)

Use-Case Specification: Forgot password

# Use-Case Name

## Brief Description

The forgot password use case for Book Alley allows users to recover their account when they forgot their password by using their recovery email.

# Flow of Events

## Basic Flow

1. The user clicks on the "Forgot Password" button on the login page.
2. The system prompts the user to enter their recovery email address.
3. The system validates the entered email address to ensure it is associated with a registered account.
4. If the email is valid, the system proceeds to the next step; otherwise, an error message is displayed.
5. An email containing the reset link is sent to the user's registered email address.
6. The user checks their email and clicks on the provided password reset link.
7. The link directs the user to a secure page on the website where they can reset their password.
8. The user enters a new password and submits the form.
9. The system updates the password and the user receives a confirmation message that their password has been successfully reset.
10. The user can now log in using the new password.

## Alternative Flows

### Invalid email address

* If the entered email address is not registered in the system, an error message is displayed, prompting the user to enter a valid email address.

### Expired or invalid reset link

* If the user clicks on an expired or invalid password reset link, the system should notify the user and provide them with the option to request a new reset link.

### Account lockout

* Implement security measures to prevent misuse, such as temporary account lockout or CAPTCHA, if there are multiple unsuccessful password reset attempts.

# Special Requirements

## Security

* The entire process must be conducted over a secure, encrypted connection to protect sensitive user information.
* The password reset token should be securely generated, unique for each user, and expire after 24 hours.
* The system should protect against common attacks, such as cross-site request forgery (CSRF) and mass assignment leading to accounts being stolen.
* The system should implement rate-limiting mechanisms to prevent abuse or brute-force attacks on the password reset functionality.

## Accessibility

* All interactive elements, such as form fields, buttons, and links, should be easily navigable using keyboard tabbing and keyboard shortcuts.
* The password reset functionality should be compatible with screen readers, ensuring that all form fields, instructions, error messages, and success messages are properly announced.

## Performance

* The forgotten password functionality should have optimal response time to provide a seamless user experience.
* The system should be designed to handle a potentially large number of password reset requests.
* Optimize the size of emails or notifications sent during the password reset process to minimize bandwidth usage and reduce delivery time.

## Regular backup

* Implement a regular backup system for the user database. Protects against data loss and ensures data recovery in case of system failures.

# Preconditions

## Internet connectivity

* The user's device should have a working internet connection to access the website

## User is registered

* The user attempting to use the "Forgot Password" functionality must be registered and already have an account

## Valid email address

* The user provides a valid email address associated with their account during the password recovery process.

## System availability

* The forgot password page should be up and running

# Postconditions

## Password reset successful

* After successfully completing the password reset process, the user's account password should be updated in the system.
* The new password should be immediately activated and allow the user to log in to their account.

## Notification sent

* A confirmation email should be sent to the user, notifying them that their password has been changed.
* The confirmation message can also be displayed on the password reset page..

## Expired link

* If a reset password link expires or becomes invalid, the system should inform the user and provide an option to request a new reset link.

## User feedback

* Provide clear and user-friendly feedback messages throughout the process, indicating the status of each step (e.g., whether the email was sent successfully, whether the reset link is valid, etc.).

## Security audit

* Conduct periodic security audits to ensure that the "Forgot Password" functionality remains secure and is not susceptible to common vulnerabilities, such as account enumeration or token misuse.

# Extension Points

## Custom email templates

* Allow administrators or users to customize the content and appearance of the password reset email. This way, the email can be tailored to match the branding of the e-commerce site or include additional instructions.

## Integration with external identity providers

* Provide an extension point to integrate with external identity providers or authentication services. This allows users to reset their password through methods like social login or third-party authentication services.

## Integration with Password Management Tools

* Enable integration with popular password management tools, allowing users to easily reset their password and update it within their password manager.

## Two-Factor Authentication (2FA)

* Provide an option to enable two-factor authentication for the forgotten password process.

## Multi-Channel Password Reset

* Extend the password reset functionality to support multiple channels, such as SMS or voice-based password reset options in addition to email.

## Logging and analytics hooks

* Integrate extension points for logging and analytics. This enables administrators to track and analyze user interactions with the "Forgot Password" feature, helping in identifying potential issues or user behavior patterns.