# Functional Requirements Document (FRD)

Feature: Customer Login

Project: ParaBank QA Automation

Author: Baseeil Elwali

Date: August 10, 2025

Version: 1.1

## 1. Feature Overview

The Customer Login feature enables registered ParaBank customers to securely access their banking accounts using their username and password. It serves as the primary entry point for account-related operations, making its reliability, usability, and security essential to customer trust and regulatory compliance.

## 2. Objectives

- Validate the secure and accurate login process.

- Ensure proper handling of invalid or missing credentials.

- Confirm compliance with accessibility and usability standards.

- Test for resilience against common security threats (e.g., SQL Injection, XSS).

- Verify proper logging and audit trail creation for login attempts.

## 3. Functional Requirements

|  |  |
| --- | --- |
| ID | Requirement Description |
| FR1 | The login form must display Username and Password fields. |
| FR2 | A “Login” button must be provided to submit credentials. |
| FR3 | Credentials must be validated against the backend user database. |
| FR4 | Valid credentials must redirect the user to the account overview page. |
| FR5 | Invalid credentials must trigger a descriptive error message. |
| FR6 | A “Forgot login info?” link must navigate to the account recovery page. |
| FR7 | A “Register” link must navigate to the new user registration page. |
| FR8 | The login form must be fully operable via keyboard navigation. |
| FR9 | The password field must mask all entered characters. |
| FR10 | All login attempts must be recorded in the audit log. |
| FR11 | Accounts must be temporarily locked after 5 consecutive failed login attempts. |
| FR12 | The login page must be responsive on desktops, tablets, and mobile devices. |
| FR13 | The login form must perform client- and server-side input validation (e.g., empty fields, whitespace-only input). |
| FR14 | The system must sanitize inputs to prevent SQL Injection and XSS attacks. |
| FR15 | Session tokens must be securely generated and invalidated upon logout. |

## 4. Test Cases

|  |  |  |
| --- | --- | --- |
| TC ID | Test Case Description | Expected Result |
| TC01 | Login with valid username and password | User is redirected to account overview |
| TC02 | Login with valid username and invalid password | Error message: “Invalid username or password” |
| TC03 | Login with invalid username and valid password | Error message: “Invalid username or password” |
| TC04 | Submit login form with empty fields | Validation message prompts user to enter credentials |
| TC05 | Submit login form with whitespace-only input | Validation message prompts user to enter valid data |
| TC06 | Click “Forgot login info?” link | Redirects to account recovery page |
| TC07 | Click “Register” link | Redirects to new user registration page |
| TC08 | Attempt login with SQL injection payload in username or password | Input rejected, error message shown |
| TC09 | Attempt login with XSS script in username or password | Input sanitized, no script execution |
| TC10 | Enter password and verify masking | All characters hidden as ● or \* |
| TC11 | Navigate form using only keyboard | All fields and buttons accessible in logical order |
| TC12 | Access login page from mobile device | Page adapts to screen size with proper layout |
| TC13 | Attempt login after 5 failed attempts | Account locked message displayed |
| TC14 | Verify audit log entry after login attempt | Entry recorded with timestamp, username, and status |
| TC15 | Verify session management after successful login | Session token generated and invalidated on logout |

## 5. Security Considerations

- Enforce HTTPS for all login traffic.

- Sanitize and validate all user inputs on client and server.

- Protect against SQL Injection, XSS, and brute force attacks.

- Securely manage authentication tokens and session cookies.

## 6. Dependencies

- Active user account records in the database.

- Functional authentication service.

- ParaBank web application UI framework.

- Audit logging infrastructure.