Secure Online Banking Systen

User Guide

Group 13

Mar 28, 2020

Contents

1. Overview of the User Guide
   1. Purpose of the User Guide
   2. How to use the Guide
   3. Requirements
2. Overview of the Secure Banking System
   1. Introduction to the System
   2. Security Features of the System
3. Online Banking Interfaces
   1. Login
   2. Internal User
      1. Tier-1 Employee
      2. Tier-2 Employee
      3. Tier-3 Employee
   3. External User
      1. Customer
      2. Merchant
4. Limitations and Assumptions

1 Overview of the User Guide

* 1. Purpose of the User Guide

This User Guide is designed to assist the online bank users, including bank employees and customers, to be familiar with the developed secure online banking system. Step by step, we will show each page and functionalities for different users. Moreover, the security features will be explained and described in detail to assure user’s safety to use the online banking system.

* 1. How to Use the Guide

In chapter 1.3, the guide will describe the requirements to use the online banking system.

In chapter 2, an overview of the secure banking system will be introduced including the security features.

In chapter 3, the guide will describe the use for users with different roles, including tie-1 employ, tier-2 employ, tier-3 employee, customer and merchant. First of all, the login page, which is shared by all users, will be described. Then user can look into different specific section according to his/her role to grasp the design, feature and functionality of the user’s subsystem.

Some limitations are described in chapter 4.

If user has any further question or concern, a technical help and support team can be reached at [sbsgroup15@gmail.com](mailto:sbsgroup15@gmail.com).

* 1. Requirements

The secure banking system is deployed on the AWS which has all necessary hardware to host the server. The user just needs qualified operation system and browser to visit the server as a client.

1. Operating System Requirements

* Apple OS X or above
* Ubuntu 14.05 or above
* Microsoft Windows 7 or above

1. Browser Requirements

* Safari 6.2.9 or above
* Internet Explorer 10 or about
* Mozilla Firefox 40.0 or above
* Google Chrome 45.0 or above

1. Overview of the Secure Banking System
   1. Introduction to the System

The secure banking system is hosted on a virtual machine and be 24\*7 available to customers and employees online through a web browser.

User-friendly interfaces are designed to the frontend. Logic and security realizations are implemented in the backend. Database is initiated and maintained to support multi-functions of the system. Two kinds of users are hypothesized to use the system, categorized as internal users and external users. The internal users can be classified into 3 groups with gradually higher privileges, i.e. tier-1 employees, tier-2 employees, and tier-3 employees. The external users include individual customers and merchants/ organizations. Three kinds of accounts, i.e. checking account, saving account and credit accounts, are designed as in the real world. Basic functionalities are developed to allow users to create, view, modify, close accounts, debit, credit, and transfer money, request, grant and decline authorization, view log-in and transaction history or bank statement in a secure environment.

For security concerns, all valid and approved transactions are captured in Hyperledger blockchain platform to guarantee safety along with the traditional security measurements taken including Secure Sockets Layer/ Transport Layer Security, Public Key Infrastructure, One Time Password, Data Masking and Hashing techniques. Besides the account number, associated emails and phone numbers are valid Personal ID as well for money sending. Technical account access is realized for employees with proper privilege to assist customers in troubleshooting and maintenance.

The banking system is developed by comprehensively considering real-world functionalities and potential malicious security attacks.

* 1. Security Features of the System

Security is the core of the online banking system. To ensure the online transactions are secure and the online banking system is able to crack various potential attacks, including session hijacking, cross scripting, SQL injection, excessive privilege attack, privilege elevation attack and malicious login control, several key security functionalities are equipped and implemented on this online banking system. A list of security features is shown below.

1. Public Key Certificates

A public key infrastructure (PKI) allows users of the Internet and other public networks to engage in secure communication, data exchange and money exchange. This is done through public and private cryptographic key pairs provided by a certificate authority.

1. One Time Password

A one-time password (OTP) is an automatically generated numeric or alphanumeric string of characters that authenticates the user for a single transaction or login session. Virtual keyboard is implemented to validate highly sensitive transactions.

1. Multiple Users Simultaneous Accessibility

By deploying on Amazon Web Service, the online banking system can be accessible to multiple users at the same time.

1. 24\*7 Accessibility

By deploying on Amazon Web Service, the online banking system can be accessible to visit 24\*7.

1. Malicious Login Control Prevention

Locking out accounts after a defined number of incorrect password attempts for a specific duration is an efficient protection against a brute force malicious login attack.

1. Session Management

A unique session key is generated by SSL’s support via HTTPS as part of the encrypted conversation. By keeping a session for each user, our online banking system can maintain state about a series of request from the same user across some period of time.

1. Data Masking Technique and Hashing Algorithms

Sensitive fields of database are protected by data masking technique and hashing algorithms.

1. Log on Sign-in History

User’s sign-in history on the date and time is kept in a log to track potential suspicious behavior.

1. Hyperledger Blockchain Platform

All valid and approved transactions are captured in Hyperledger blockchain platform to secure online banking business

.

1. Other Necessary Defense Strategies
2. Online Banking Interfaces
   1. Login

Login page is the entry on online banking system. Users including internal employees and external customers need to log into the system by entering his/her registered user name and password shown in Fig. 1.

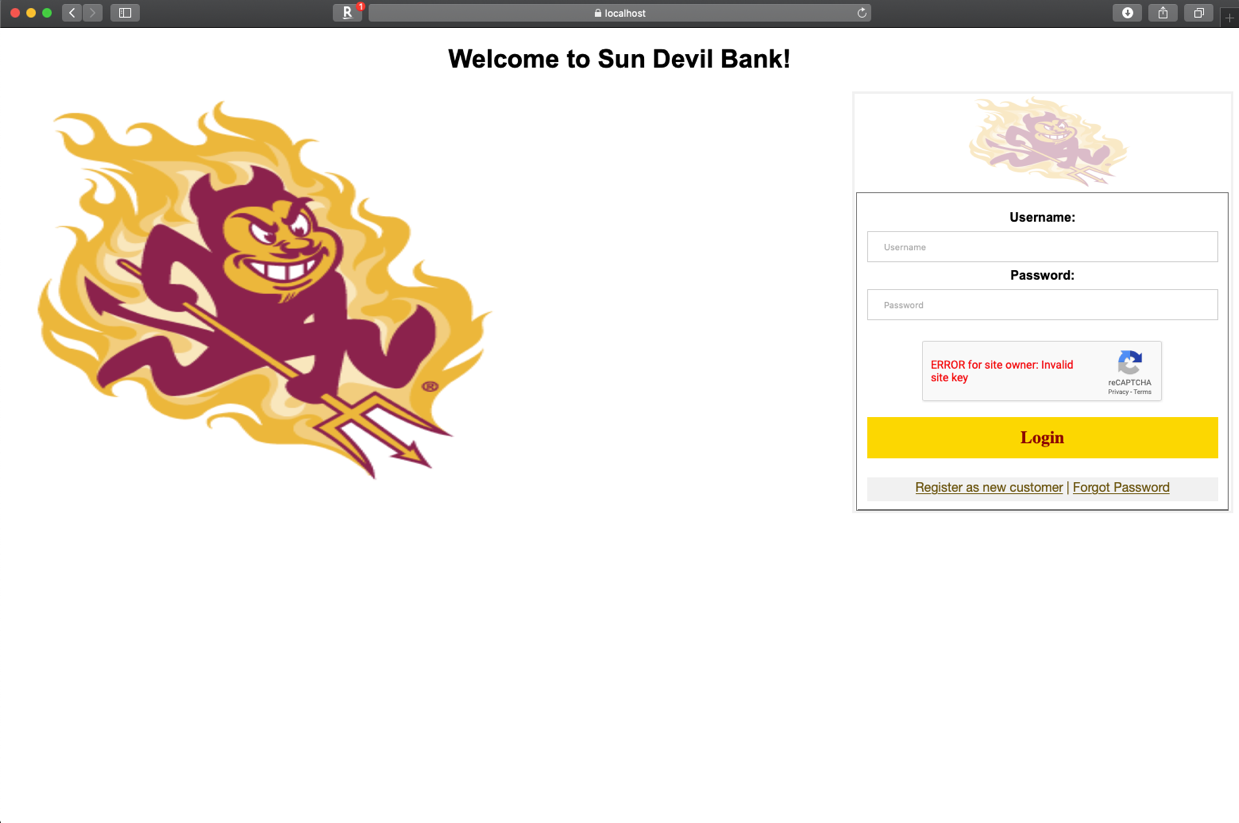


Fig. 1 Login Page

If this is your first time using the system, you can create your external user account information on the Registration Page (Fig. 2) by clicking the “Register as new customer” button on the Login Page. The required information includes Customer Type (Individual, Merchant), Desired UserName, Email, Desired Password, Confirm Password, First Name, Middle Name, Last Name, Address 1, Address 2, Phone Number, DOB (Date of Birth), SSN (Social Security Number), City, Province, Zip Code. Moreover, two security information is required for account recovery in the future. Here, you are required to input the answers to “What is your childhood nickname?” and “Who was your childhood hero?”. Meanwhile, you can erase all the information put already by clicking the “Reset” button at the bottom of the form. After inputting all the required blanks, you finish registering a new external user by clicking “Register” button at bottom.

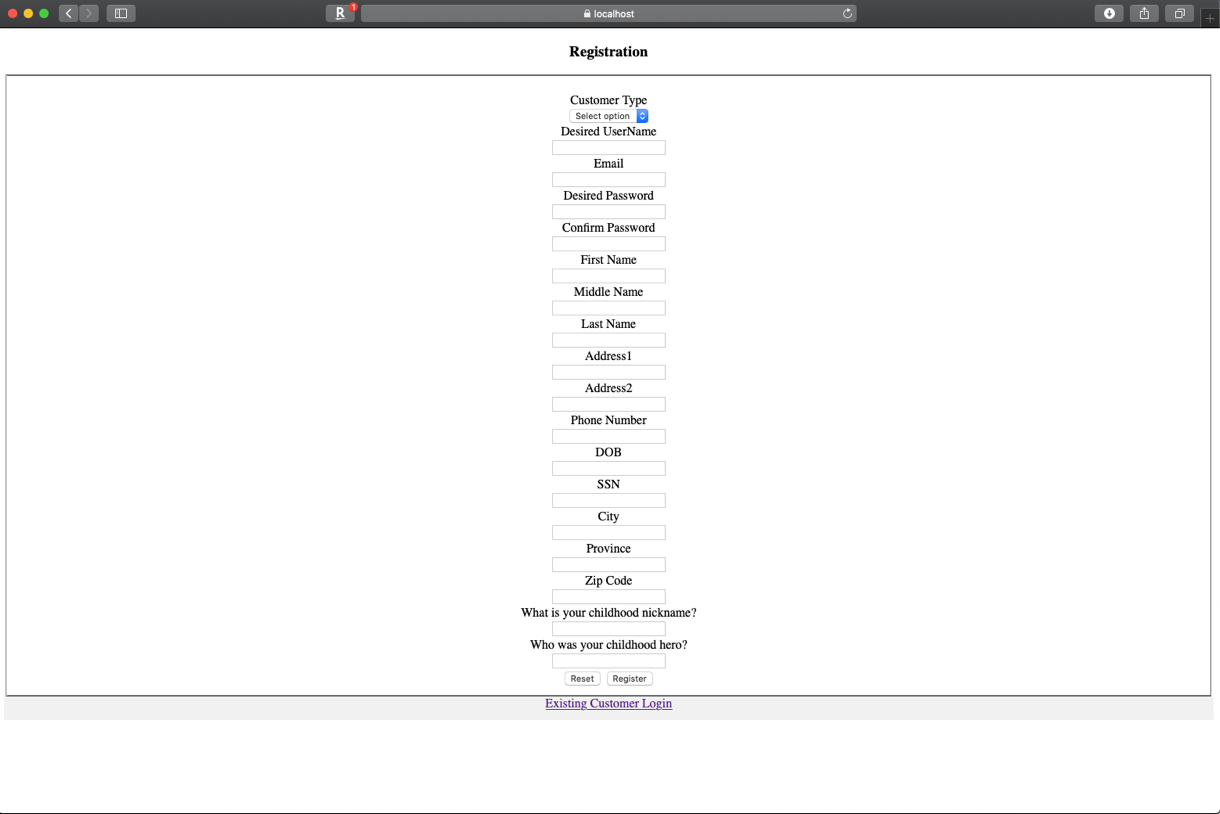


Fig 2 Registration Page

Any existing user, who forget his/her password, can log into the system with One Time Password by clicking “Forgot Password” button in Fig. 1. The Forgot Password Page is shown in Fig. 3 where you enter your user name, request a One Time Password to temporally log into the system.

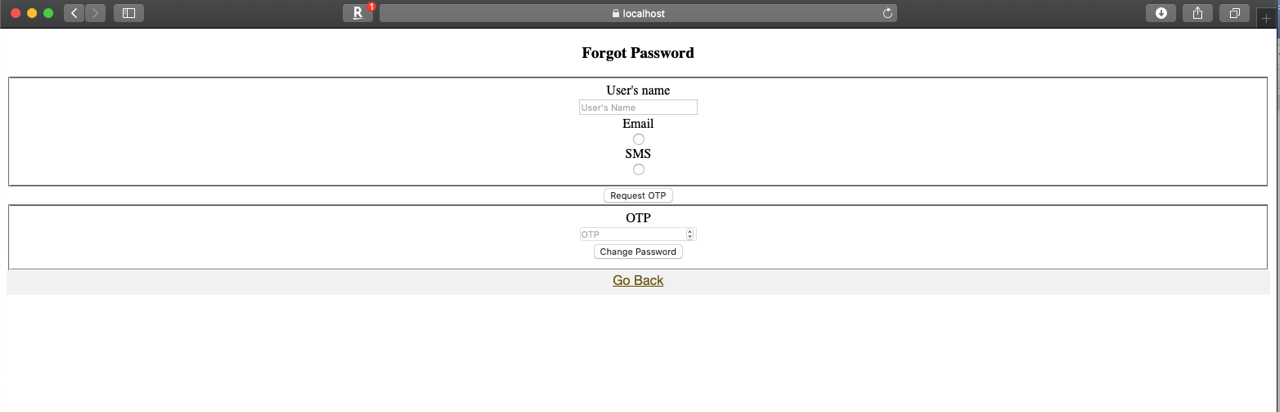


Fig 3 Forgot Password Page

Several security measures are taken to ensure the safety of system users. First of all, copy/past function is prohibited in all pages of the system. Second, CAPTCHA is implemented on the Login Page to prevent robot attack. Third, One Time Password is implemented with virtual login keyboard in Forgot Password page to prevent relay attack. Fourthly, if the account is inactive for a period of time, the system frozen and any further click will lead to logging out to the Login page.

* 1. Internal User

There are 3 kinds of internal users, including tier-1 employee, tier-2 employee, and tier-3 employee with increasing privileges.

* + 1. Tier-1 Employee

The Tier-1 Employ’s Dashboard is shown in Fig. 4-1. From the dashboard, tier-1 employ can approve/decline non critical transaction (<$1000) as in Fig 4-2, create non critical transaction as in Fig. 4-3, issue cashier cheque as in Fig.4-4, deposit cash cheque as in Fig. 4-5, deposit money as in Fig. 4-6, withdraw money in Fig. 4-7, view customer accounts in Fig. 4-8, change password in page 4-9, view appointments of the day in page 4-10.

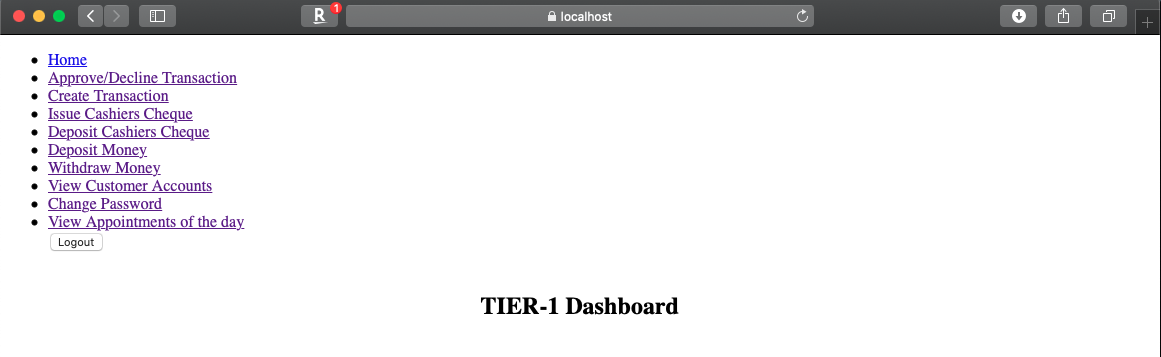


Fig. 4-1 Tier-1 Employee Dashboard

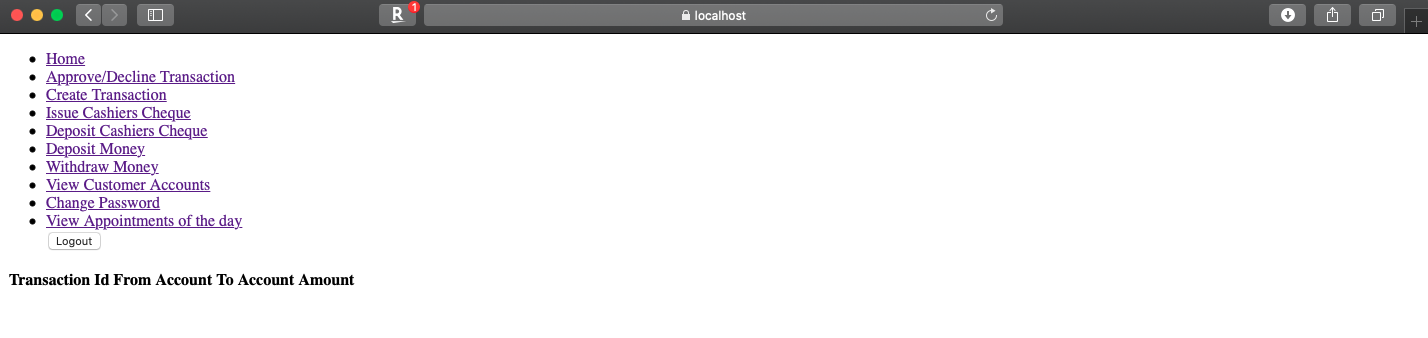


Fig 4-2 Approve/Decline Transaction Page

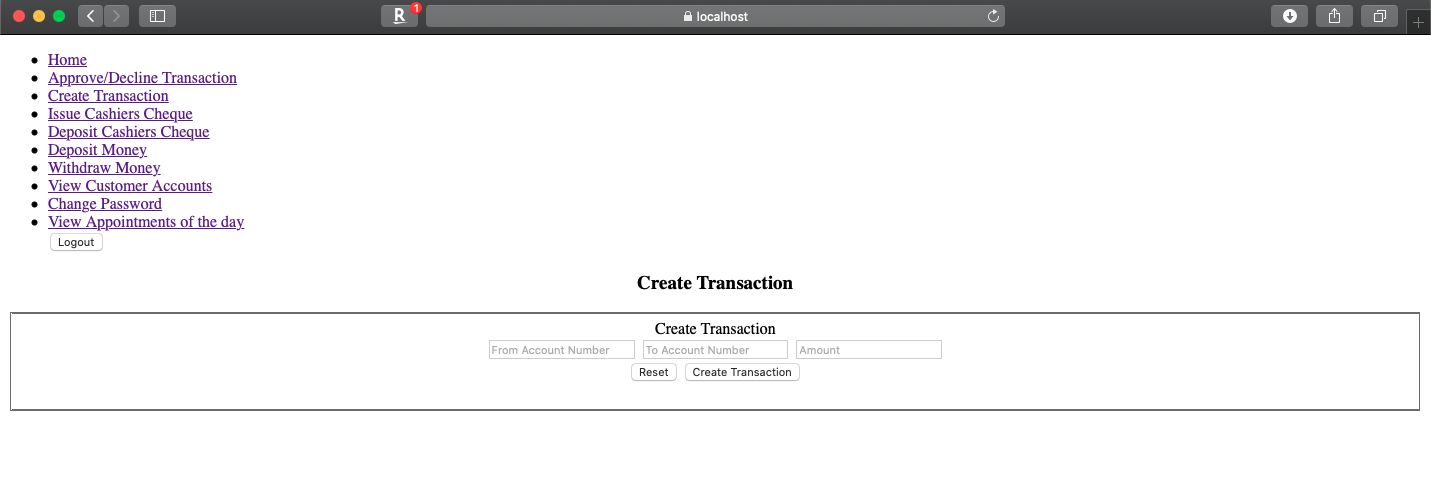


Fig 4-3 Create Transaction Page

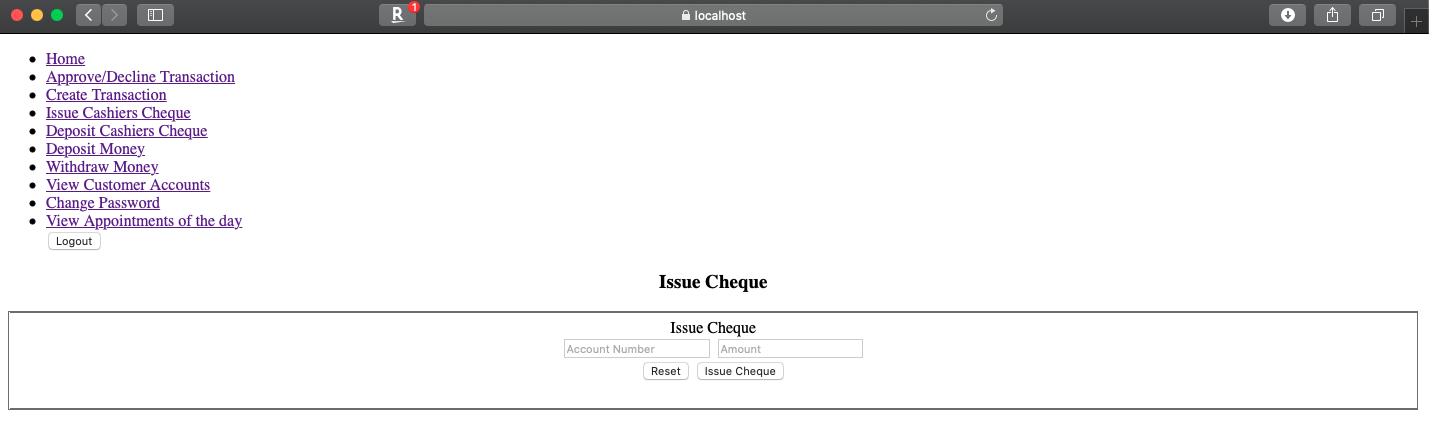


Fig 4-4 Issue Cashier Cheque Page

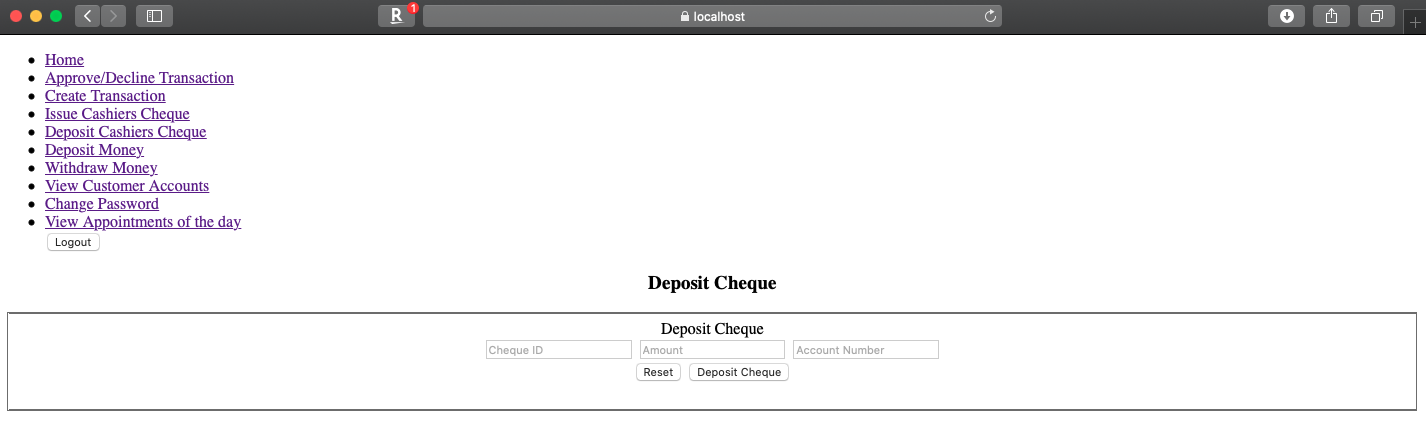


Fig 4-5 Deposit Cashier Cheque Page

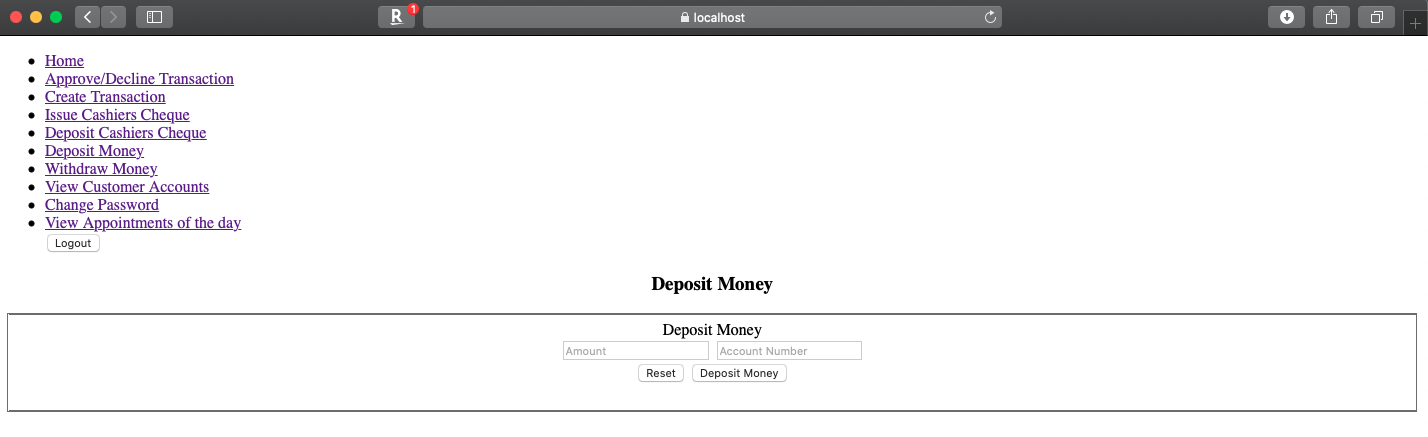


Fig 4-6 Deposit Money Page

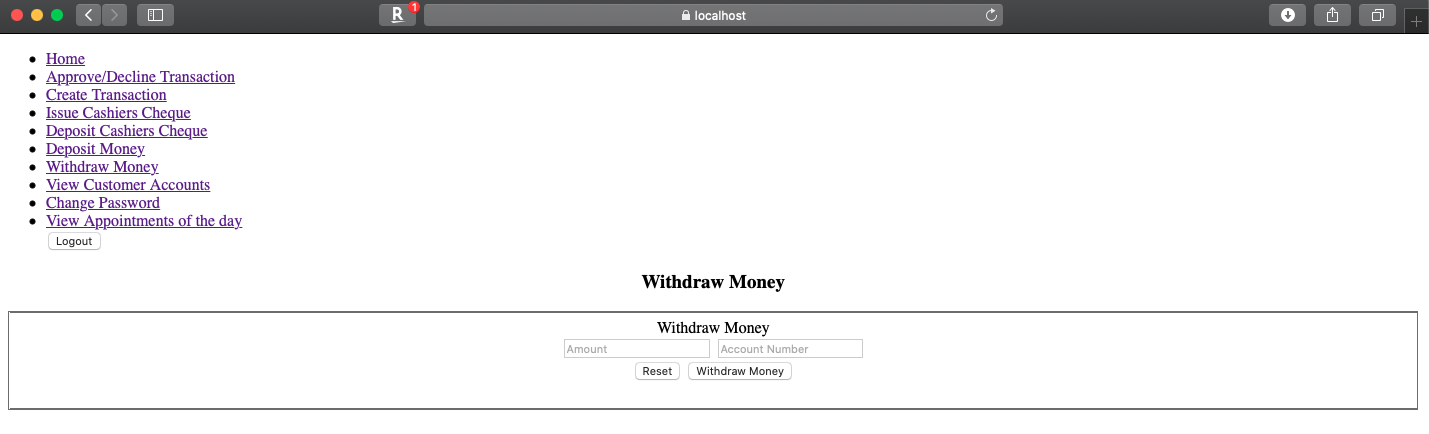


Fig 4-7 Withdraw Money Page

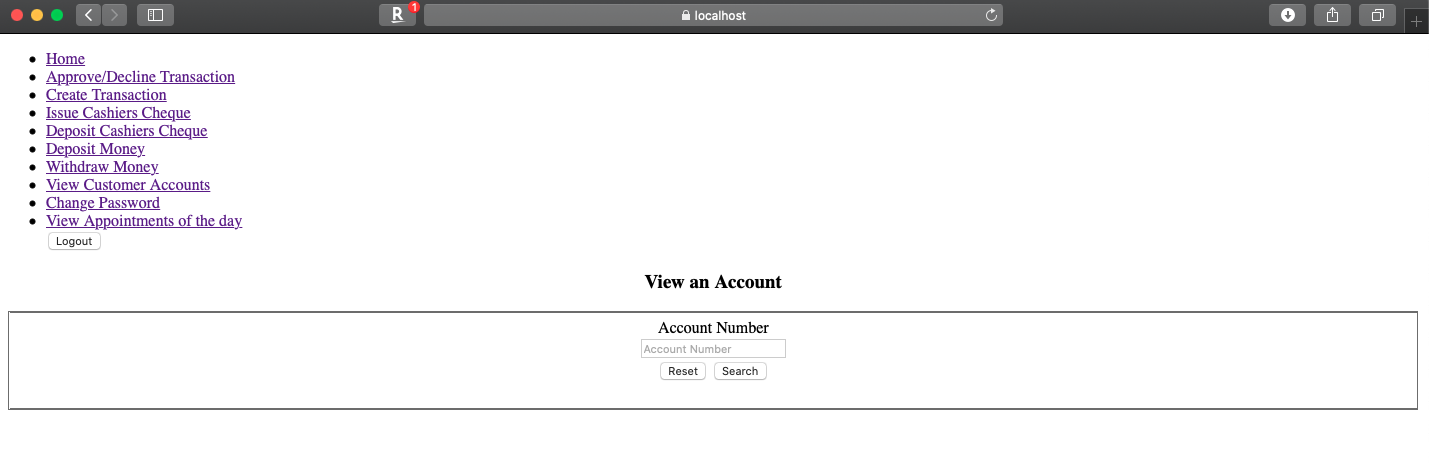


Fig 4-8 View Customer Account Page

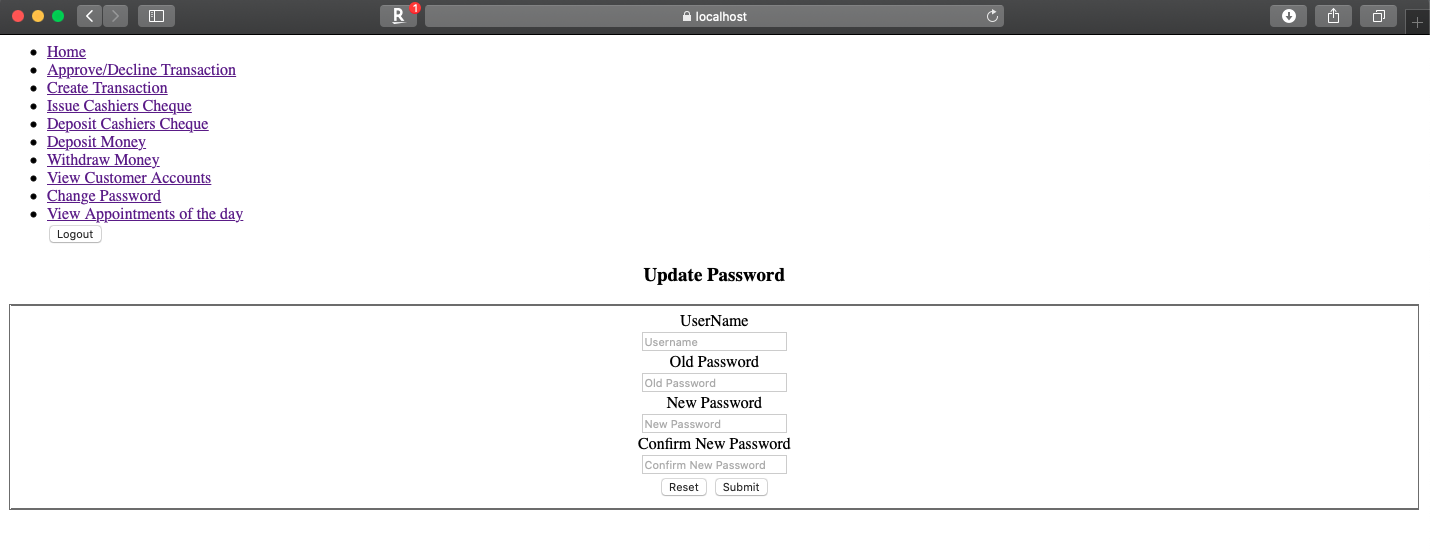


Fig 4-9 Change Password Page



Fig 4-10 View Appointment of the Day Page

* + 1. Tier-2 Employee
    2. Tier-3 Employee
  1. External User
     1. Customer

Fig.7-1 shows the dashboard of customer account. Customer can find the account information including savings account, checking account, and credit account. For each account, customer can deposit/withdraw money (Fig 7-1-1), view recent transactions (Fig 7-1-2), and transfer funds(Fig 7-1-3).

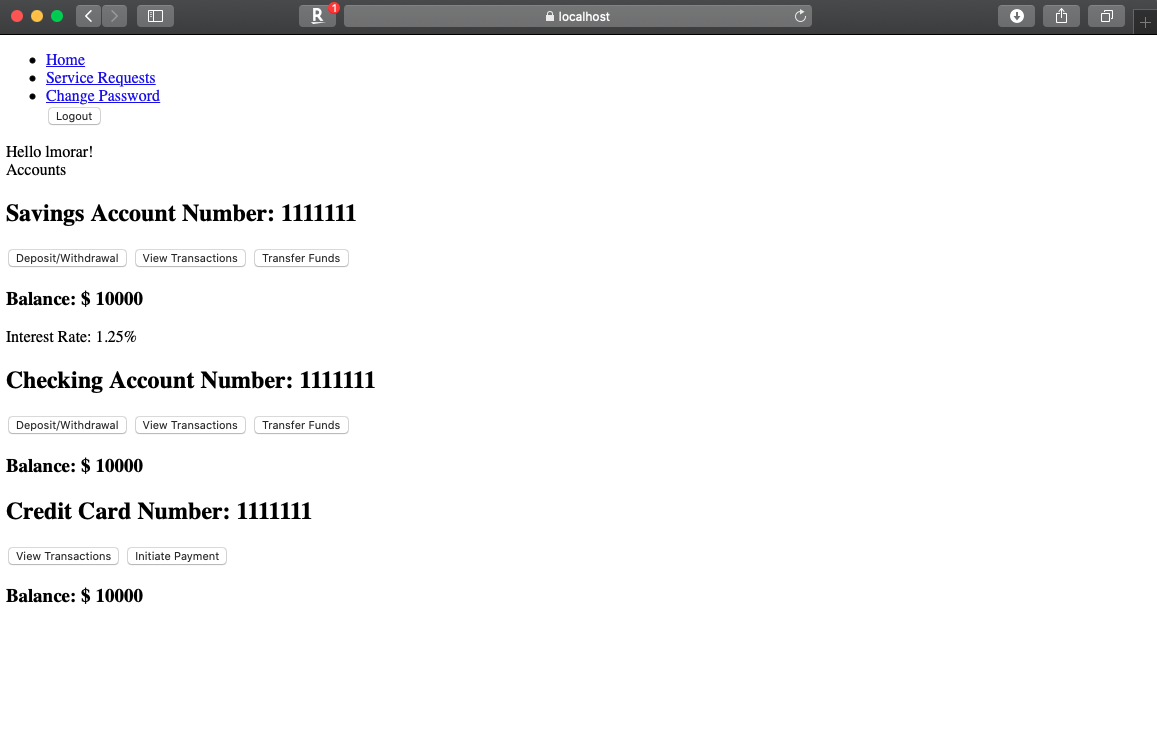


Fig 7-1 Customer Dashboard Page

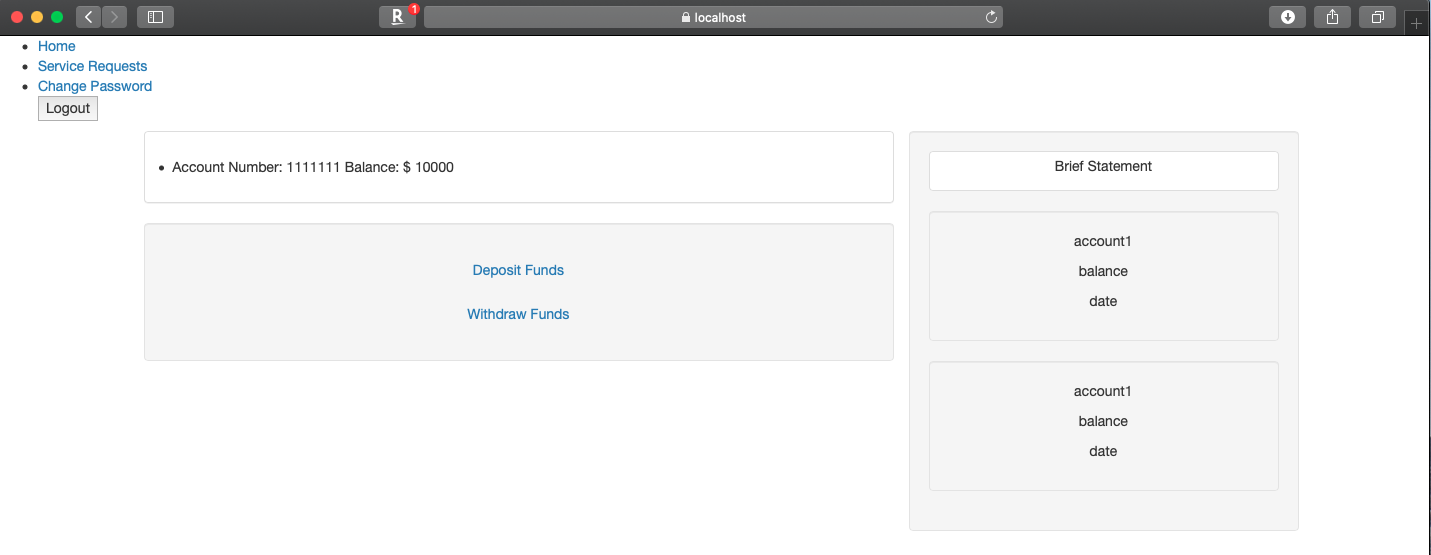


Fig 7-1-1 Deposit/ Withdraw Money Page

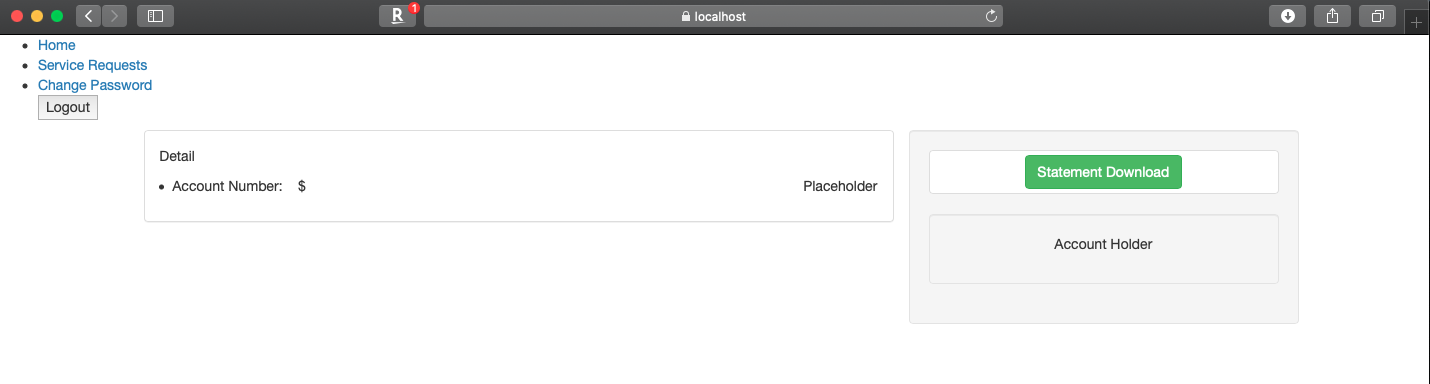


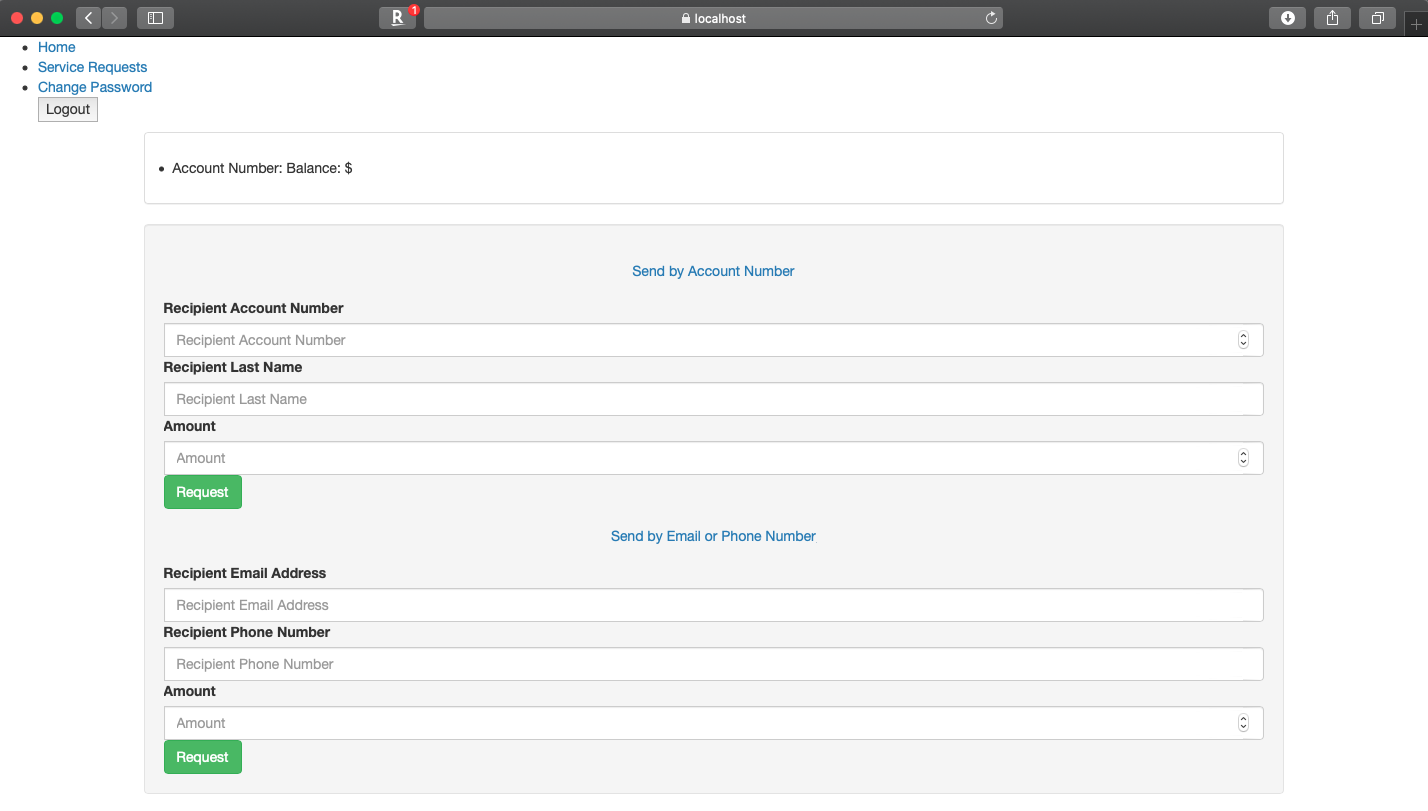
Fig 7-1-2 View Transactions Page

Fig 7-1-3 Transfer Funds Page

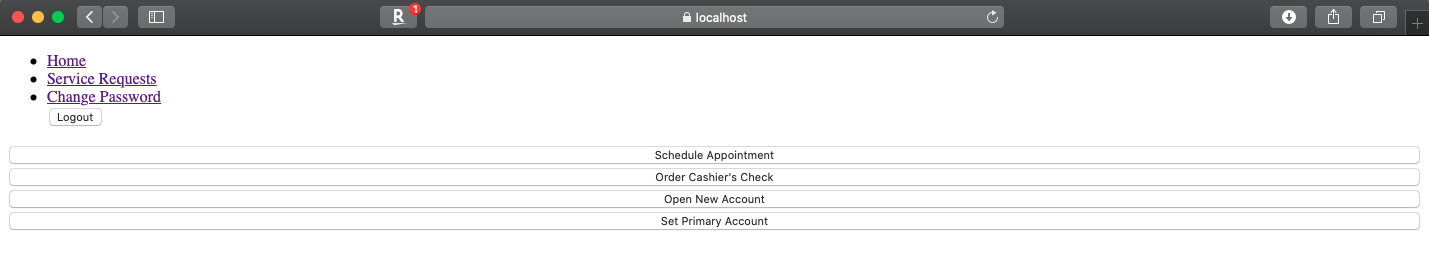


Fig 7-2 Service Request Page

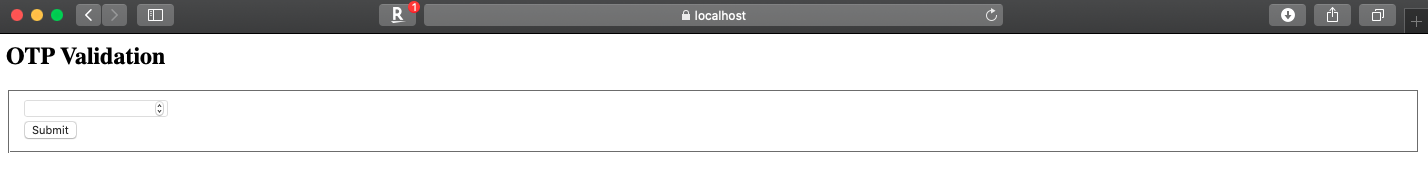


Fig 7-2-1 Schedule Appointment Page

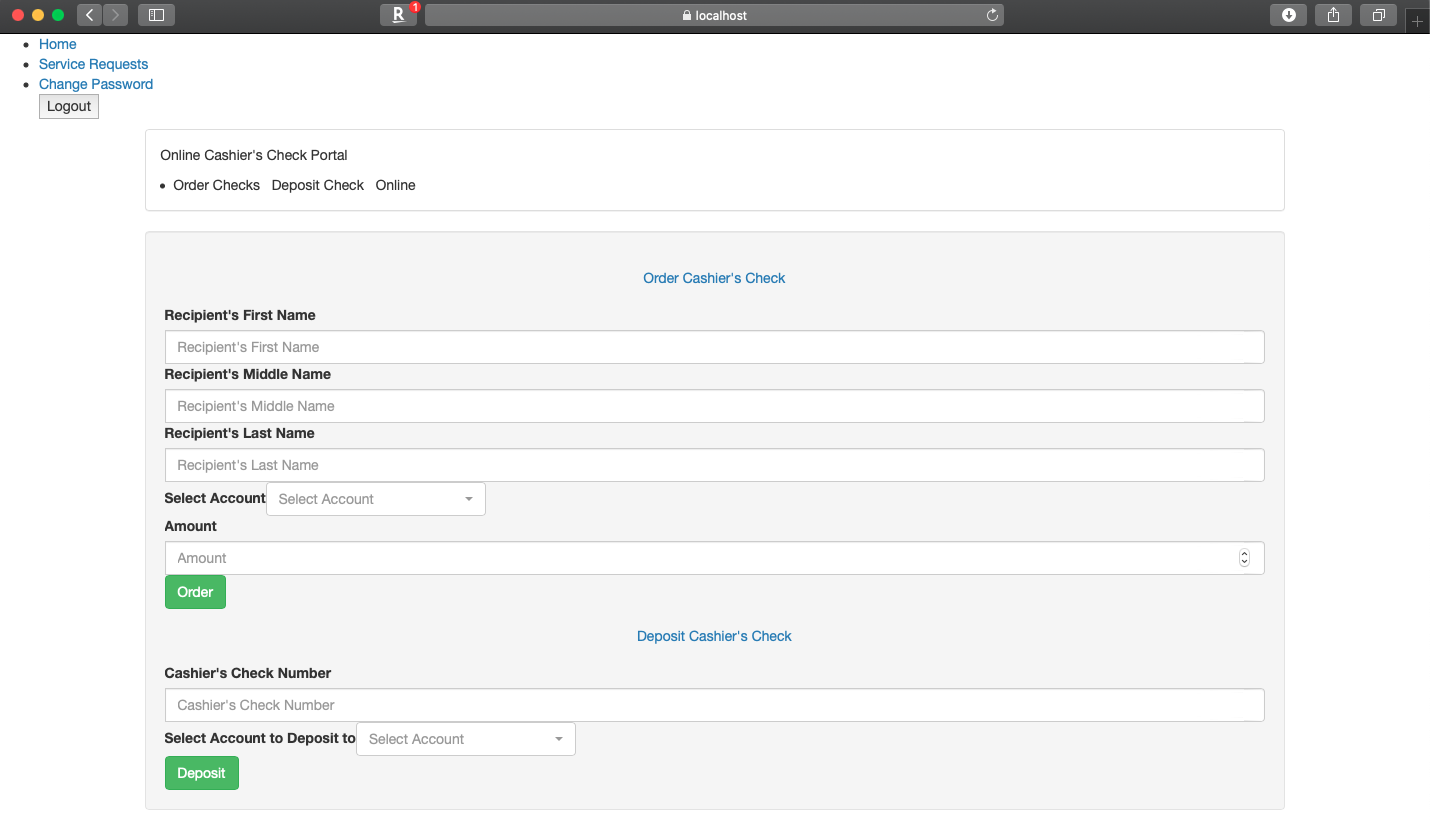


Fig 7-2-2 Order/Deposit Cashier’s Cheque Page

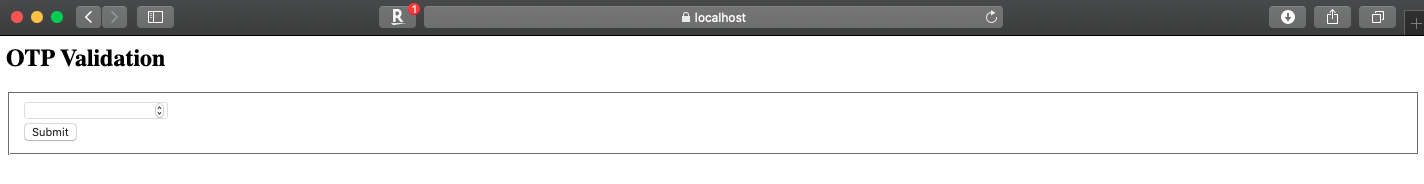


Fig 7-2-3 Open New Account Page

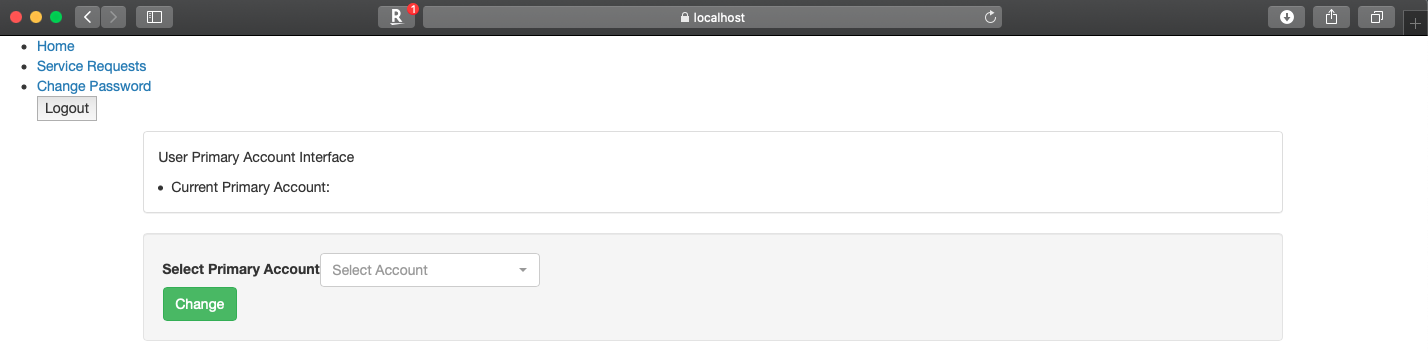


Fig 7-2-4 Set Primary Account Page

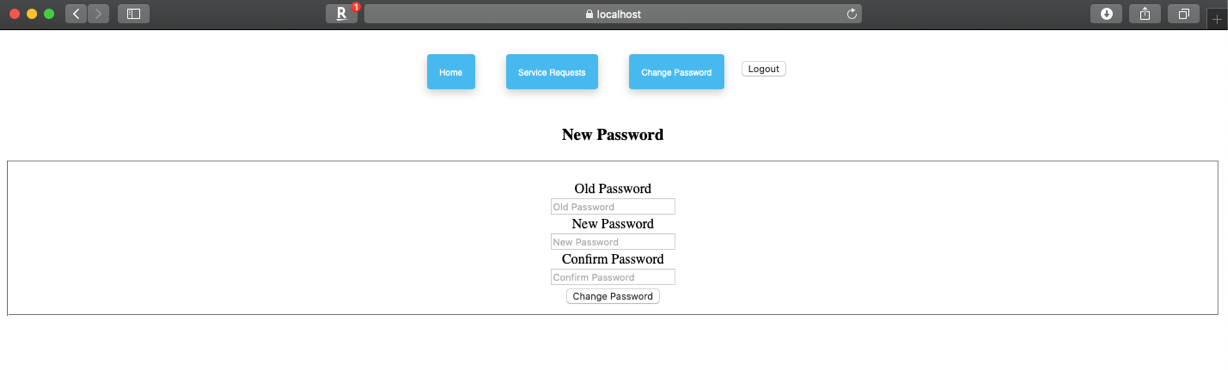


Fig 7-3 Change Password Page

* + 1. Merchant

1. Limitations