Secure Programming
Threat Modeling

Submitted By
Team w3w:
Albayda, Giodeelyn
Celadeña, Harvey
Coloma, Juan Paolo
Corpuz, Danica Christine
Nieva, Patricia Hera
S23

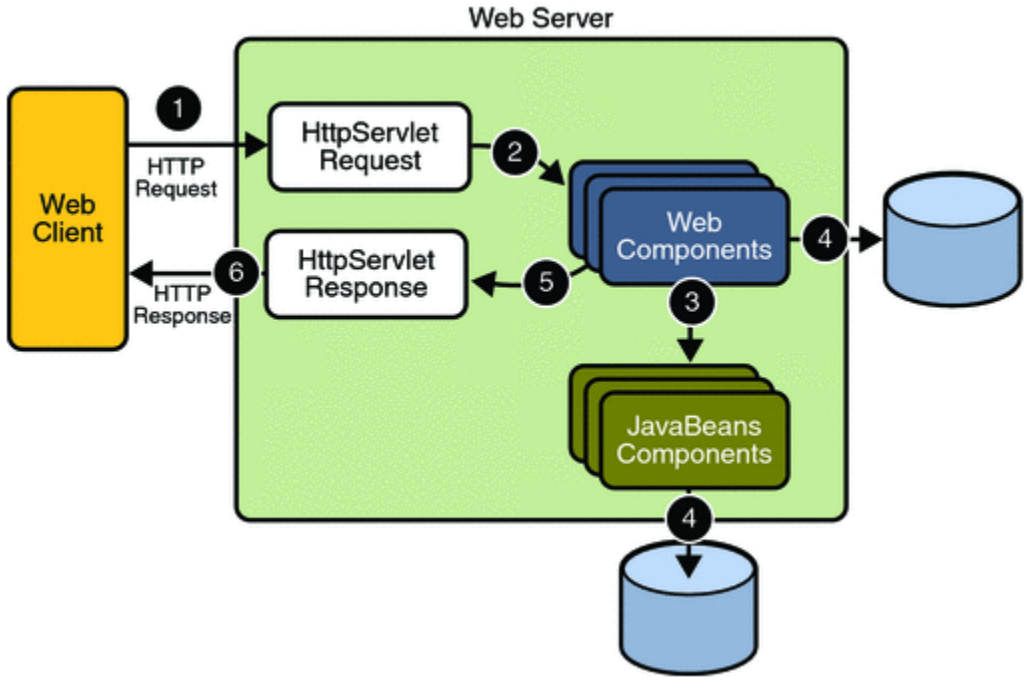
Submitted To:
Ms. Katrina Solomon
November 3, 2014

I. Security Objectives

- Protect customer account details and customer credit history.
- Ensure that the application is available 99.99 percent of the time.
- Prevent unauthorized users from modifying product catalog information, especially prices.
- Ensure that only authorized people are allowed to access the critical information of the application.

II. Application Overview

a. End-to-End Deployment Scenario



Flow

Using the IDE, we created a web application that would start a servlet container like Apache Tomcat to be able to deploy our web application. When a browser is opened, it sends an HTTP request, where this contains the HTTPServletRequest and the HTTPServerResponse that allows access of the information in an HTTP request and allows manipulation of values while having this. These values would then be stored in the database depending on how the code works. An HTTP session will be alive once the user opened the web application, it is usually 30 minutes before it runs dead. Servlets are used, to be able to embed to the HTML pages.

Services

Easy navigation

This website is intended to help the customer navigate and purchase items with ease. As the customer navigates on through the page, he/she should be able to go to each kind of product with ease because the main options or categories are presented in its menu.

Simple Shopping

Once the desired products are in the cart, payment can be simply made by credit card. After a successful order, the customer will be informed about the current status of his/her order. A tracking number will also be received.

Secure Shopping

The website would be having HTTP header protections and POST methods to prevent attacks.

b. Roles

- Administrator, Managers and Customers can view and edit their own account information
- Administrator can create but cannot edit product and accounting manager accounts
- Administrator has the ability to unlock accounts of locked users
- Administrator can view all the essential activities of the website
- Customers can view and purchase products
- Customers are capable of writing reviews on the products that they bought
- Customers are capable of creating their own accounts
- Customers are capable of adding and removing products from their shopping carts
- Customers and Managers have the option to contact the Administrator if their accounts are locked
- Customers are allowed to track their orders
- Product Managers can add, edit, view, delete product information
- Product Managers are allowed to restock products
- Only the Accounting Manager can view sales report and filter based on preferences(day, week, month, year, product)

c. Key Scenarios

Legend:

- **Key Features**
  - **Key Scenarios**

- Create Customer Account
  - The user chooses the “Register” from the “Account” options.
  - User inputs all necessary fields asked and submits
  - The system checks if password and confirm password are the same and if required fields are filled up
  - If both password matches, the system will redirect the user to the account’s billing/shipping address information and successfully created an account

- Create Manager Account
  - The administrator must be logged in
  - The administrator chooses the “Register Manager” from the “Account” options.
  - Administrator inputs all necessary fields asked and submits
  - The manager can use his/her account

- Change Password
  - User is logged in
  - The user selects the “Change Password” option
  - User inputs the old password once and the new password twice and submits
  - The system checks if the old password matches with the one in the database
  - The system then checks the new password and the retyped password if they are the same
  - If both password matches, the system will redirect the user to the “My Account” whole page

- Edit Account Information
  - User is logged in
  - The user selects the “Edit” option
  - The user changes the necessary information he/she wanted to change
  - User chooses the “Save Changes” option and the system will redirect the user to the “My Account” whole page.

- Login
    - The user chooses the “Login” from the “Account” options.
    - User inputs login information needed
    - The user will be logged in and the system will redirect the user to the “Home” page.

- Edit Billing/Shipping Address
    - Customer is logged in
    - Customer is in the Edit Account Information page
    - Customer selects the “Edit” option in the Billing/Shipping Addresses area
    - The Customer changes the necessary information in the billing/shipping addresses
    - The Customer selects the “Save Changes” option and the system would update the following information in the “My Account” page

- Edit Credit Card Information
    - Customer is logged in
    - Customer is in the Edit Account Information page
    - Customer selects the “Edit” option in the Credit Card Information area
    - The Customer changes the necessary information in the Credit Card Information
    - The Customer selects the “Save Changes” option and the system would update the following information in the “My Account” page

- Add Product to Shopping Cart
    - Customer is logged in
    - Customer searches product catalog based on his preferences
    - Customer selects an item
    - Customer then chooses the size of the desired product in the options
    - The Customer selects the “Add to Shopping Cart” option and the item will be added to the shopping cart of the Customer

- Remove Product from the Shopping Cart
    - Customer is logged in
    - Customer selects the “My Shopping Cart” option in the top menu and system will redirect to the Shopping Cart page

- Customer chooses the “Remove” in the product he/she wishes to remove from the Shopping Cart
- The system will now update the shopping cart page to see that the product has been removed from the list

- Search Product

  - Customer is logged in
  - Customer can input the name of the product or can choose within the category in the menu
  - The system will generate a list of products

- Purchase Products

  - Customer is logged in
  - Customer goes to the “My Shopping Cart” page
  - Customer selects the “Secure Checkout” option and will be redirected to the payment page
  - Customer will choose which payment method to use
  - Customer inputs necessary information for payment
  - After the Shopping Cart submits, he/she will be redirected back to the Account page

- Track Order

  - Customer is logged in
  - The Customer selects the “Order Tracking” option from the Account menu
  - The system will pop up an overlapping page and prompts the Customer to enter his/her email and the order id number
  - Customer inputs his/her email and the order id of the order he/she wants to track
  - Customer selects the “View Order Stats” option
  - The system will send the order details whether it has been delivered or still delivering to the email he/she input earlier

- Write Review
  - Customer is logged in
  - Customer purchased a product
  - System will prompt if the user wants to add a review for the item
  - Customer’s review will appear every time the customer views the product information.

- Edit Review
    - Customer is logged in
    - Customer selects the “View Products Bought” option
    - Customer selects a product and the system will prompt his transaction details and the review he wrote
    - Customer clicks “Edit Review” button
    - Customer edits his review
    - System will verify if the user wants to save the changes
- View Activity Log
    - Administrator is logged in
    - Administrator selects the “View Activity Log” option
    - Administrator may choose to filter the activity logs according to day, week, month, year.
- Restock Product
    - Product Manager is logged in
    - Product Manager selects the “View Products” option
    - System will display the products and the number of stocks left
    - Product Manager selects the product he/she wants to restock
    - Product Manager will specify how many products he/she will restock
    - System will ask confirmation from the Product Manager by asking if the Product Manager is sure. If the Product Manager says yes, the system will ask for his password; otherwise, transaction will be discarded
    - System verifies the password and if the password is correct, it will redirect the Product Manager to the “View Products” page
- Add Product
    - Product Manager is logged in
    - Product Manager chooses “Add New Product” option
    - System will display a form about the product which the Product Manager must fill up
    - System verifies if all the necessary information are filled up. If yes, the system will ask the Product Manager to review the information he filled up then asks for

his password there are no corrections. If no, the system will just disregard the transaction
    - System will authenticate the Product Manager. Product Manager will be redirected to the form just in case he/she wants to add another product

- Edit Product Information

    - Product Manager is logged in
    - Product Manager chooses “View Products” option
    - Product Manager searches for the product he/she wants to edit
    - After searching for the product, the Product Manager chooses the “Edit Product Information” button
    - The system will display a form containing the current information regarding the product. The Product Manager changes the information he/she wants to alter
    - The system will ask the Product Manager to review the information he/she placed. If there are no more corrections, the system will verify the Product Manager by asking for his/her password
    - System checks if the password is correct
    - The System will redirect the Product Manager to the “View Products” page

- Remove Product

    - Product Manager is logged in
    - Product Manager chooses the “View Products” option
    - The system will display all the products stored in the database
    - Product Manager searches for the product he/she wants to remove
    - Product Manager selects the product and chooses the “Remove Product” option
    - The System will ask if the Product Manager is sure if he/she really wants the product to be deleted from the database
    - If the Product Manager chose yes, the system will verify the Product Manager by asking for his password
    - The system will verify if the password is correct
    - The Product Manager will be directed to the page where the system will display all the products in its database

- View Sales

    - Accounting Manager is logged in
    - Accounting Manager chooses the “View Sales Report” option

    - Accounting Manager chooses the option on how he/she wants to see the Sales Report

- Contact Administrator

    - User is locked because of numerous number of failed attempts logging in
    - User will be asked by the system to contact the administrator
    - User will fill up the form by either placing his/her username or e-mail address
    - The system will verify if such user exists
    - The information will be sent to the administrator

- Unlock Account

    - Administrator is logged in
    - Administrator selects the "View Locked Accounts" option
    - Administrator selects the accounts he/she needs to unlock
    - The system verifies the Administrator by asking for his password
    - User's account will be unlocked
    - Administrator will be redirected to the "View Locked Accounts" page to unlock other users' account

d. Technologies

- Website Design and Functionalities: HTML, CSS, JavaScript, SQL, JQuery, OWASP ESAPI
- Database - keeps tracks of the activity logs
    - keeps track of the products according to their type
    - keeps track of the orders
    - keeps track of the transactions
    - keeps track of the accounts of their registered users (Customers, Managers, Administrator)
- Email - used for authentication purposes.
- Credit Card Transactions - commonly used for online transactions using a credit card.
- Firewall (anti-viruses)

e. Application Security Mechanisms

- The Application is secured by the OWASP ESAPI library.
    - Website requires a minimum length of 8 for the password of the account

- Website requires customers to register and login in order to verify user details to proceed to billing and shipping information.
- When the user attempts to login multiple times with a wrong password, his/her account will be locked. By this, the user will have to contact the administrator so that his/her account will be unlocked.
- When the customer enter his/her credit card information, the application will use a secure checkout to protect the user's information. Once the customer decided to purchase the product, his/her credit information will be encrypted and will be send to a third-party service.
- HTTP header X-Xss-Protection is enabled to prevent reflected cross site scripting attack.

III. Application Decomposition

a. Trust Boundaries

- The first trust boundary is the perimeter firewall because it transfers the qualified information from the Untrusted Internet to the trusted data center.
- The second trust boundary is the web server which limits the access of users to databases. Because of this, any user can access the product catalog and add items to their shopping cart but only registered users are trusted to purchase the items.
- The boundary between the application and a third-party service. It trusts the service's identity. The application uses a secure and safe standard when paying through online.

b. Data Flows

- An anonymous user registers an account. The name must be less than 50 characters in length and must not include special characters while the password requires having a minimum of 8 characters in length. The user is also required to input his/her email address and username. He/she is not encouraged to input his/her username same as to his/her name or email address. The user needs to have a valid username and e-mail address, in case that his username and/or e-mail address is invalid, the system will ask him to place a valid one. After the registration met the requirements, it will then be passed as a parameter of a function and will be stored inside the database. This transaction will also be logged into the system's database.

- The administrator will create an account for the accounting and product manager. The name must be less than 50 characters in length and must not include special characters. The administrator will be using a temporary username and password

and the data access component checks and passes the information as a parameter to a function to be stored inside the database. After the account was made, the manager will be notified about his/her account details and he/she is required to change the password and other information he wishes to within 24 hours. This transaction will also be logged into the system's database.

- When the customer or manager logs to his/her account, the username and password of the user will be passed as a parameter to a function. His/her information will be checked if it matches the information inside the database. If so, her information will be send back to the user and he/she will going to have a unique session id. However, it will also be checked in the database if the user attempted to log for more than 5 logins. If this happens, he/she will not be provided with his/her own unique session id and he/she will have to contact the administrator. This transaction will also be logged into the system's database.

- When the user changes his/her password, he/she needs to provide the new password and retype his/her old password for verification. The passwords are stored temporarily on the web server. After that, it will be passed as a parameter to a function and will be send. The database will checked if it matches its stored password and the old password that was typed by the user. If the two matches, the database will remove the old password, and store the new password. This transaction will also be logged into the system's database.

- The user decides to edit his/her account information, he/she has the opt to change all the information and is temporarily stored on the web server. Once he/she is finished, it will be passed in a function to reach the database and in order to change his old information with the new ones, the system will ask the user to enter his password for verification. The database will just overwrite the information stored in it with the information from the user's session. This transaction will also be logged into the system's database.

- The Customer browses the items from the product catalog. From the catalog page, it calls the data access component to call the function so that the items from a particular category will be displayed into the webpage. The customer can add items to their shopping cart which is temporarily stored on the web server. It will then be stored on the user's account into the database server. When the user decided to purchase the item, he will be directed to a secure checkout which uses HTTPS. The customer chooses the credit card he/she will use to pay, he/she will have to provide his card information to verify and authenticate his account. The

application uses a secure standard to protect the cardholder and encrypts the data to the third-party service. The system would log the transaction made.

- In addition, the customer submits a search string. The search string limited to 50 characters in length. The application processes the input and will be passed to the data access component. It will call the function that will return the information needed from the database into the webpage.

- The product manager adds product. He/she will input all the necessary information based on the product. The information should not exceed up to 20 characters in length except for summary which could have up to 50 characters and the year should only be 4. The price and number of stocks may vary so it will be limited up to 5. After that, it will be passed as a parameter of a function from the data access component to store the data into the database. This transaction will also be logged into the system's database.

- If the product manager wants to edit the information of a specific product, he needs to search for the product from the list of all the products gathered from the system's database. The information should not exceed up to 20 characters in length except for summary which could have up to 50 characters and the year should only be 4. The price and number of stocks may vary so it will be limited up to 5. After that, it these pieces of information will be passed as a parameter of a function from the data access component overwriting the data about that product into the database. This transaction will also be logged into the system's database.

- The Product Manager is also capable of removing the product from the system's database. If he wants to remove a product, he needs to search for the product he wants to delete. After selecting, the product information will be passed as a parameter of a function from the data access component removing the product from the system's database. This transaction will also be logged into the system's database.

- In addition, the Product Manager can view product's information. He needs to search for a keyword regarding or filter the product according to his preferences. This will be passed as a parameter of a function from the data access component which will retrieve products that answers the query of the Product Manager.

- If the customer bought an item successfully, the system will ask the customer wants to write a review for the product. If the customer agrees, he will be redirected to a form in which he needs to fill up. After filling up the form, the

information will be passed as a parameter of a function from the data access component to store the data about that product into the database. Same process goes with the scenario of the user wanting to write a review for the product he bought some time ago. This transaction will also be logged into the system's database.

- After several failed attempts of logging in, the user's account will be locked. In order for the user's account to be unlocked, he needs to contact the Administrator. The system will ask the user's e-mail address and/or username and these will be passed as a parameter of a function from the data access component which will be stored into the database. Once the Administrator accessed the list of the locked accounts from the database, he has the capability of unlocking the account of these users. This transaction will also be logged into the system's database.

- The Administrator views the activity log of the system. He chooses from the preferences available to view the activity logs. Based from the preference he chose, it will be passed as a parameter of a function from the data access component. This will retrieve the list of logs accordingly and display on the web page.

- Accounting Manager views the sales report of the store. He chooses from the preferences available to filter the sales report. Based from his choice, it will be passed as a parameter of a function from the data access component to search the database with the pieces of information needed. The report retrieved from the database will then be displayed on to the web page.

c. Entry Points

- Logon page. Accessible to all Internet users. Validated by using client-side and server-side validation controls, together with common validation library.
- Enter the website itself via the web browser (port 80 or 443). The user will type the domain name and it will allow the user to select from the countries that they locally support.

d. Exit Points

- Once the customer was able to finalize the products he will buy and chose to proceed with the payment method, he needs to verify his credit card information. The customer may either use the credit card information he placed upon

registration or provide another credit card number. The customer's credit card information will be sent to the bank's server to confirm if the credit card really exists or not.

IV. Threats

- Attacker could create a same looking website and redirects the user from the legitimate url to a fake website.
- Attacker sends fake emails and provides authentic-looking website and url that asks to login and enter personal and financial information.
- Attacker could steal login information by virtual listening in on to the user while using the unsecured WiFi network.
- Attacker creates botnets to launch denial-of-service attacks to keep the real website down, making it unavailable to users.
- Attacker could create a bogus account and use stolen credit card information to allow him to make transactions.

V. Vulnerabilities

- Clear text credentials are passed between the Web server and database server.
- Replay attack. It is an attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.

USE CASE DIAGRAM AND SCENARIOS

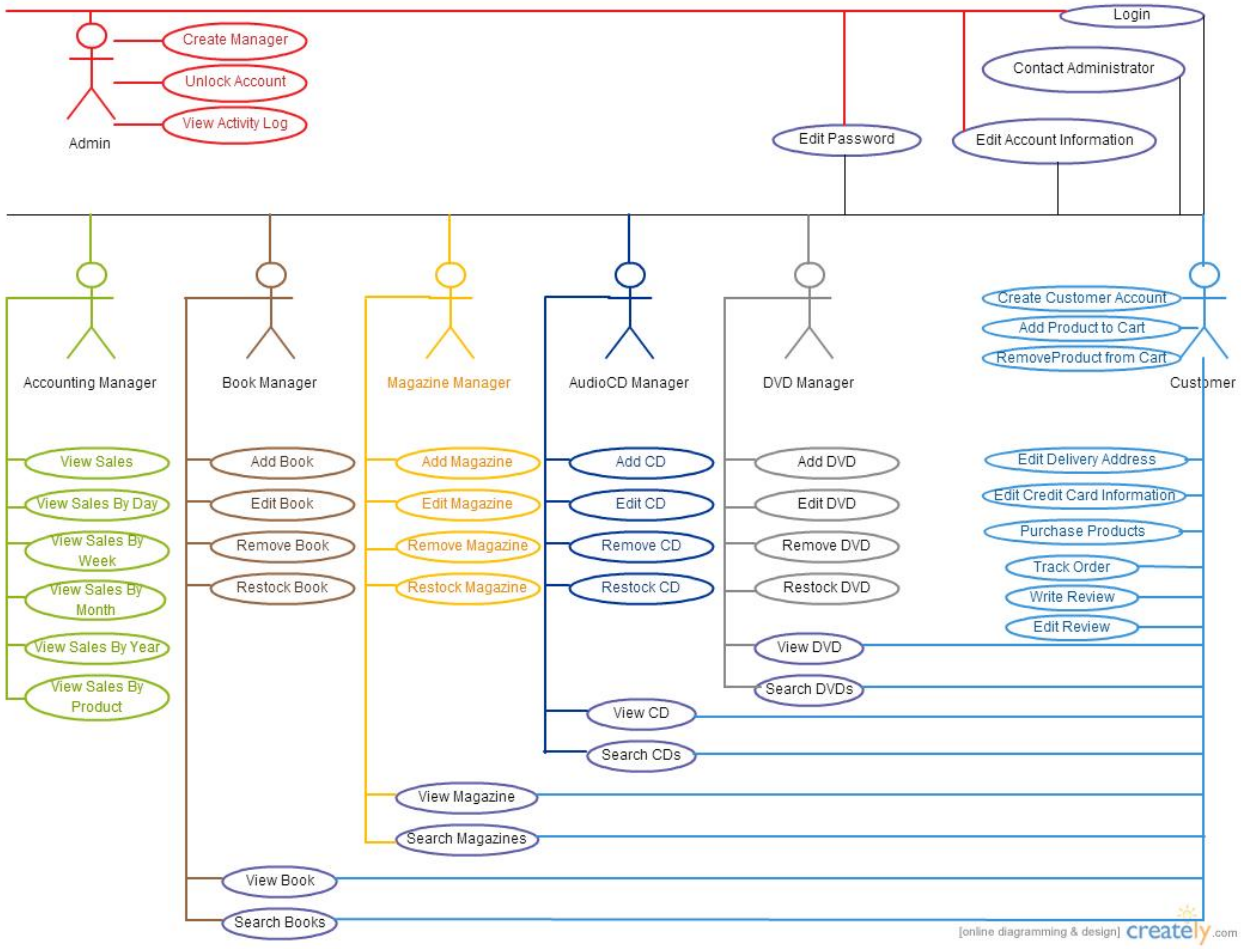


Diagram Description: Foobar Bookshop System

Use Case: Create Customer Account

Main Flow:

1. The user chooses the "Register" from the "Account" options.
2. User inputs all necessary fields asked and submits
3. The system checks if password and confirm password are the same and if required fields are filled up
4. If both password matches, the system will redirect the user to the account's billing/shipping address information and successfully created an account

Exceptional Flow:

1. If the customer inputs incorrect information they will prompted and will be asked to change it with a correct one.
2. If the customer inputs a password that does not correspond to the confirm password it will prompt the user to input the correct password.
3. If the customer inputs a password that is less than 8 characters, he/she will not be allowed to create an account.

4. If the customer tries to use important information (username, e-mail address) that's being used by a user, the system will highlight the field specifying that the information placed is not available and will be asked to change it with an unused one.

Use Case: Create Manager Account
Main Flow:
1. The administrator must be logged in
2. The administrator chooses the "Register Manager" from the "Account" options.
3. Administrator inputs all necessary fields asked and submits
4. The manager can use his/her account

Exceptional Flow:
1. If the administrator decides not to make a new account while inputting the fields asked, he/she may choose the cancel button.
2. If the administrator decides not to make a new account upon system confirmation, he/she may choose the "no" button.
3. If the administrator inputs a temporary password that is less than 8 characters, he/she will not be allowed to create a manager account.

Use Case: Change Password
Main Flow:
1. User is logged in
2. The user selects the "Change Password" option
3. User inputs the old password once and the new password twice and submits
4. The system checks if the old password matches with the one in the database
5. The system then checks the new password and the retyped password if they are the same
6. If both password matches, the system will redirect the user to the "My Account" whole page

Exceptional Flow:
1. If the user inputs his old password as his new password, the system will tell him to change the password.
2. If the password chosen doesn't match the minimum requirements specified, the system will tell the user to change the password.
3. If the user decides not to change his password, he needs to choose the "cancel" button which will leave no changes in his account.

Use Case: Edit Account Information
Main Flow:
1. User is logged in
2. The user selects the "Edit" option
3. The user changes the necessary information he/she wanted to change
4. User chooses the "Save Changes" option and the system will redirect the user to the "My Account" whole page

Exceptional Flow:

1. If the user decided not to change any information, he/she may choose the cancel option which will leave no changes in his/her account information.
2. In case the user decided to change his/her e-mail and/or username and if the e-mail and/or username he placed is currently unavailable, the system will inform the user that it is unavailable and will ask him/her to change if he still wants to edit his/her e-mail address and/or username.

Use Case: Login
Main Flow:
1. The user chooses the "Login" from the "Account" options.
2. User inputs login information needed
3. The user will be logged in and the system will redirect the user to the "Home" page

Exceptional Flow:
1. If the user entered wrong login information, the system would redirect the user in the same login page.
2. If the user tried to login multiple times, the system would lock his/her account and prompts to contact the administrator to unlock his/her account.

Use Case: Edit Billing/Shipping Address
Main Flow:
1. Customer is logged in
2. Customer is in the Edit Account Information page
3. Customer selects the "Edit" option in the Billing/Shipping Addresses area
4. The Customer changes the necessary information in the billing/shipping addresses
5. The Customer selects the "Save Changes" option and the system would update the following information in the "My Account" page

Exceptional Flow:
1. The Customer decided not to change any information regarding his billing/shipping address; he may choose to select the "Cancel" button while filling up the form.
2. In case that the Customer finished filling the form and proceeds to verify the information, if he decided not to continue editing his billing/shipping address he may choose the "No" button if the system asked him if he wants to save the changes.

Use Case: Edit Credit Card Information
Main Flow:
1. Customer is logged in
2. Customer is in the Edit Account Information page
3. Customer selects the "Edit" option in the Credit Card Information area
4. The Customer changes the necessary information in the Credit Card Information
5. The Customer selects the "Save Changes" option and the system would update the following information in the "My Account" page

Exceptional Flow:

1. If the Customer inputs an invalid credit card number, the system will prompt and ask the user to change the credit card number.
2. If the Customer decides not to change his credit card information while filling up the form, he may choose the "Cancel" button to discard the form.
3. If the Customer decides not to change his credit card information but chose the "Save Changes" button, the system will ask the customer again if he's sure if he really wants to change his credit card information.

Use Case: Add Product to Shopping Cart
Main Flow:
1. Customer is logged in
2. Customer searches product catalog based on his preferences
3. Customer selects an item
4. Customer then chooses the size of the desired product in the options
5. The Customer selects the "Add to Shopping Cart" option and the item will be added to the shopping cart of the Customer

Exceptional Flow:
1. If the Customer decides not to add the product to his shopping cart, he may choose to select the "No" option when the system asks him if he's sure to add the product to his shopping cart.

Use Case: Remove Product from the Shopping Cart
Main Flow:
1. Customer is logged in
2. Customer selects the "My Shopping Cart" option in the top menu and system will redirect to the Shopping Cart page
3. Customer chooses the "Remove" in the product he/she wishes to remove from the Shopping Cart
4. The system will now update the shopping cart page to see that the product has been removed from the list

Exceptional Flow:
1. If the Customer decides not to remove the product from his shopping cart, he may choose to select the "No" option when the system asks if he's sure to remove the product from his shopping cart.
2. If there are no products inside the shopping cart, the system would display a blank page in the shopping cart page.

Use Case: Search Product
Main Flow:
1. Customer is logged in
2. Customer can input the name of the product or can choose within the category in the menu
3. The system will generate a list of products

Exceptional Flow:

1. If there are no products equivalent to the query stated by the Customer, the system will tell the customer that there are no products and will suggest other products that are related to it.

Use Case: Purchase Products

Main Flow:

1. Customer is logged in
2. Customer goes to the "My Shopping Cart" page
3. Customer selects the "Secure Checkout" option and will be redirected to the payment page
4. Customer will choose which payment method to use
5. Customer inputs necessary information for payment
6. After the Shopping Cart submits, he/she will be redirected back to the Account page

Exceptional Flow:

1. If the information specified by the customer is invalid, the system will prompt and ask the user to change these pieces of information.
2. If the customer's account is not capable of buying the products, the system will cancel the transaction and ask the customer to place valid card information that is capable of purchasing the products.

Use Case: Track Order

Main Flow:

1. Customer is logged in
2. The Customer selects the "Order Tracking" option from the Account menu
3. The system will pop up an overlapping page and prompts the Customer to enter his/her email and the order id number
4. Customer inputs his/her email and the order id of the order he/she wants to track
5. Customer selects the "View Order Stats" option
6. The system will send the order details whether it has been delivered or still delivering to the email he/she input earlier

Exceptional Flow:

1. If the customer decides not to track his order anymore, he may choose the "Cancel" option and he will be redirected to the "Home" page.
2. If the customer places invalid track number, the system will prompt and tell the customer that the track number placed is invalid and will be asked to place a valid track number.
3. If there are no track orders yet for that customer, the system would display "Please order first so you can be able to track".

Use Case: Write Review

Main Flow:

1. Customer is logged in
2. Customer purchased a product

3. System will prompt if the user wants to add a review for the item
4. Customer's review will appear every time the customer views the product information.

Exceptional Flow:

1. If the customer bought the product and chooses not to write a review, he will be redirected to the "Home" page after purchasing the product.
2. If the customer decides to write a review for a previously bought product, he needs to go to his "View Products Bought" page and from there, selects the product he wants to write a review.

Use Case: Edit Review

Main Flow:

1. Customer is logged in
2. Customer selects the "View Products Bought" option
3. Customer selects a product and the system will prompt his transaction details and the review he wrote
4. Customer clicks "Edit Review" button
5. Customer edits his review
6. System will verify if the user wants to save the changes

Exceptional Flow:

1. If the Customer decides not to edit his review for the product, he needs to choose the "Cancel" button to indicate that his current review will not be altered.

Use Case: View Activity Log

Main Flow:

1. Administrator is logged in
2. Administrator selects the "View Activity Log" option
3. Administrator may choose to filter the activity logs according to day, week, month, year.

Exceptional Flow:

1. If there are no activity logs yet for a filter, the system would display a message to inform the administrator that there are no activities yet for that specific filter.
2. If the data within the month or week is incomplete, a notification message would appear to inform the administrator that data is inaccurate due to missing dates.

Use Case: Restock Product

Main Flow:

1. Product Manager is logged in
2. Product Manager selects the "View Products" option
3. System will display the products and the number of stocks left
4. Product Manager selects the product he/she wants to restock
5. Product Manager will specify how many products he/she will restock
6. System will ask confirmation from the Product Manager by asking if the Product Manager is sure. If the Product Manager says yes, the system will ask for his password; otherwise, transaction will be discarded

7. System verifies the password and if the password is correct, it will redirect the Product Manager to the "View Products" page

Exceptional Flow:

1. If the Product Manager decides not to restock the product, he needs to choose the "Cancel" button to disregard the number of stocks he's about to restock.

Use Case: Add Product(Book/Magazine/AudioCD/DVD)

Main Flow:

1. Product Manager is logged in
2. Product Manager chooses "Add New Product" option
3. System will display a form about the product which the Product Manager must fill up
4. System verifies if all the necessary information are filled up. If yes, the system will ask the Product Manager to review the information he filled up then asks for his password there are no corrections. If no, the system will just disregard the transaction
5. System will authenticate the Product Manager. Product Manager will be redirected to the form just in case he/she wants to add another product

Exceptional Flow:

1. If the product to be added is already stored in the database, the system will tell the Product Manager that the product exists and if he still wants to proceed with the session; however, the session will just restock the product with the number of products specified by the Product Manager.
2. If the Product Manager decides not to continue adding the product to the database while filling up the form, he needs to choose the "Cancel" button to disregard the session.
3. If the Product Manager's done filling up the forma and proceeds to adding the product but then decided not to continue adding the product, he may choose "No" when asked if he's sure to add the product.

Use Case: Edit Product Information

Main Flow:

1. Product Manager is logged in
2. Product Manager chooses "View Products" option
3. Product Manager searches for the product he/she wants to edit
4. After searching for the product, the Product Manager chooses the "Edit Product Information" button
5. The system will display a form containing the current information regarding the product. The Product Manager changes the information he/she wants to alter
6. The system will ask the Product Manager to review the information he/she placed. If there are no more corrections, the system will verify the Product Manager by asking for his/her password
7. System checks if the password is correct
8. The System will redirect the Product Manager to the "View Products" page

Exceptional Flow:

1. If the Product Manager decides not to continue editing the product information while filling up the form, he needs to choose the "Cancel" button to disregard the session.

2. If the Product Manager's done filling up the form and proceeds to save the changes but then decided not to continue editing the product information, he may choose "No" when asked if he's sure to edit the product information.

Use Case: Remove Product
Main Flow:
1. Product Manager is logged in
2. Product Manager chooses the "View Products" option
3. The system will display all the products stored in the database
4. Product Manager searches for the product he/she wants to remove
5. Product Manager selects the product and chooses the "Remove Product" option
6. The System will ask if the Product Manager is sure if he/she really wants the product to be deleted from the database
7. If the Product Manager chose yes, the system will verify the Product Manager by asking for his password
8. The system will verify if the password is correct
9. The Product Manager will be directed to the page where the system will display all the products in its database

Exceptional Flow:
1. If the Product Manager decides not to continue removing the product from the database while filling up the form, he needs to choose the "Cancel" button to disregard the session.
2. If the Product Manager's done filling up the form and proceeds to removing the product but then decided not to remove adding the product, he may choose "No" when asked if he's sure to remove the product.
3. If there are no products to remove, the product manager could not then remove anything.

Use Case: View Sales
Main Flow:
1. Accounting Manager is logged in
2. Accounting Manager chooses the "View Sales Report" option
3. Accounting Manager chooses the option on how he/she wants to see the Sales Report

Exceptional Flow:
1. If there are no sales yet, the system would display a message to inform the accounting manager that there are none available sales recorded yet.

Use Case: Contact Administrator
Main Flow:
1. User is locked because of numerous number of failed attempts logging in
2. User will be asked by the system to contact the administrator
3. User will fill up the form by either placing his/her username or e-mail address
4. The system will verify if such user exists
5. The information will be sent to the administrator

Exceptional Flow:

1. If there happens to be a run-time error and the system wasn't able to send the information to the administrator, an error message should be displayed.

Use Case: Unlock Account

Main Flow:

1. Administrator is logged in
2. Administrator selects the "View Locked Accounts" option
3. Administrator selects the accounts he/she needs to unlock
4. The system verifies the Administrator by asking for his password
5. User's account will be unlocked
6. Administrator will be redirected to the "View Locked Accounts" page to unlock other users' account

Exceptional Flow:

1. If there are no accounts locked yet, the system would display a notification that there are no accounts locked yet and check again later.