CECS 491A - Section 5/6

November 1st, 2018

Business Requirements Document

[Team Spyderz]

[Product: CheckIt]

Jonathan Asencio [Project Leader] - Back End - 014245983

Alex Philayvanh - Back End - 017508814

Bryan Bare - Back End - 011741260

Kunal Patel - Front End - 013329054

Table of Contents

Introduction

Spyderz is a development team set to manage the creation of CheckIt, a web based application for price tracking and product distribution. CheckIt was conceived through a need to free up time in people lives. With growing responsibilities and less time to accomplish them, CheckIt hopes to provide people a more productive and efficient lifestyle. CheckIt will provide multiple features to different kinds of users seeking different needs for organization while shopping. It will also serve as an easy to use platform for product distributors, no matter their size. Such offered features include creating a watchlist of items that users can personally curate to their needs, automatically receiving notifications on price drops based on user set constraints. Users can create customized profiles and share such watchlists amongst friends. Businesses can also create customized profiles to post their inventory and to partner up with CheckIt to crowdsource a wanted/popular item. Users can also directly search for an items through our search bar to receive a list of prices for the searched item. Through providing a service to allow people to efficiently search product to obtain the lowest price, our goal is to help people quickly handle these tasks so they can have more time to complete the important things in their life. The target audience is anyone who has a knack for online shopping or product distribution.

Scope

The goals of our product regarding scope include to offer our features to the entirety of North America. All current residents of North America will have access to our features. If an entity outside of North America wants to use our products we will determine that based on IP and effectively block them from using our website. Along with only allowing North American residents to access our website, we will also possess initial data that includes Geography, Role Data, Permission Data, and IP addresses. Our website will use the latest version of Google's Chrome browser. Some additional requirements for the scope are as follows:

- Using SPA for our web applications
- Logs over 2 years old are archived and then deleted
- Users must be 18 years of age
- Geographic scope is all of North America
  - 1.23.186.0 - 223.197.44.239 USA ip range
  - 2.17.218.0 - 217.77.255.10 Canada ip range
  - 4.18.32.72 - 216.251.76.254 Mexico ip range
  - Further ip addresses found at https://www.bestyoucanget.com/nablock.php
  - Vpn is out of scope
- Role data includes which users have what roles within our system
  - Guest, Customer, Business, Administrator, or System Administrator
- Permission data will include individual rules and permissions each role can have
- We will also record each ip address that visits our website

Features

Core Features

Authentication

Authentication of our product will include how we must verify users. This process will be how we check to see if a user is valid to sign up for our system and use our features. Rules for verifying users include:

A. Users must be able to login and out of out website.
B. Users must be able to reset their password.

This will allow users to have access to certain features of our website. Along with our certain rules of business. Such rules and requirements that are expected from users are:

(1) Users must enter correct criteria into the login to start a session.
    (a) Valid email and password
(2) Ability to update password during a valid session
(3) Ability to log out of a system as long as their session is active
(4) Inactive users will be kicked from the server after 30 minutes of no server communication
    (a) Inactivity includes staying on the same page for more than 30 minutes or not sending any server requests within that time

Given these rules that are in place, other grounds must be set for all to work holistically. Some of this foundation that must be included is:

(1) A username must be a valid email address
(2) A password must be between 12-2000 characters.

(3) Passwords are not stored in plain text for security.

(4) A bruteforce attack should take longer than 50 years.

(5) Accounts will be disabled after 3 invalid login attempts

  (a) Users will be able to reset the password and then answer the 3 security questions to unlock the account

  (b) Admin Users have ability to manually re-enable an account besides admin accounts.

(6) Server extend session once a valid activity occurs

With this foundation laid out, our system will then be graded on certain criteria. A pass would be deemed true if the username and password are correct. A fail would be a result if the login username or password is not correct. A lockout would occur on an account if 3 failed attempts are made.

Authorization

Authorization within our system will determine what each user or guest can or cannot access or view. The one rule for authorization within our system is that the system must have user access control. Providing the system with this control will allow the system administrator to set certain constraints on user roles. For example: a regular customer cannot view the website logs. Some of the requirements that follow this rule include:

(1) Dashboard visibility will depend on having a valid session and the user role

(2) Unauthorized users will be informed of a fail access attempt

Just having these rules is not enough though. Certain constraints will be placed upon the rules as follows:

(1) Users should not be able to view, execute, or have access to things they should not have access to

(2) Users can precisely configure their access to data, website functionality and content of the system

(a) Basically they are able to remove what they don't want to see

(3) Users are required to be legal adults in their respective countries in order to access the system (Canada, Mexico, and US are 18 years old)

With these rules and constraints in place, we can successfully set and determine the access control of any users in our system.

Authorization would be successful whenever a request is made with a satisfactory permissions level. Successful authorization allows users certain access to the application based on given permissions. Should a lower ranked permission user try to access a high ranked asset, their authorization would fail.

Privacy

Privacy is a big concern when it comes to our website. Privacy will handle many legal ends for the website. As we implement privacy to our system, we are faced with two requirements:

(1) The website will have a Terms of Service (end-user license agreement)

(2) Users will have access and control of their data privacy

(a) This includes personal account information and history

These rules are set in place to both protect the user and the website from legal backlash. The broad rules do have requirements though, and they are as follows:

(1) System administrators will be able to add, update, and delete an EULA

(2) The system is unlocked to users upon accepting the EULA

Some constraints on these rules will provide greater insight to what exactly we can do and how we can set up privacy:

(1) Only one EULA is active at a time
(2) Users must consent to collection of personal information and metrics they use for the website
(3) Users can opt out of telemetry data collection at any time
(4) Users can see what type of data is being collected about them
(5) Collected user data can be deleted at anytime by deleting the user account.

These constraints are put in place to define the way privacy is maintained. The EULA is the door to our system. Should the user not accept the EULA, they cannot access the system. Privacy should only fail once a user opts out of telemetry collection or deny the EULA.

Creation

Creation within our system includes the creation of user accounts. There are two requirements involved in creating an account:

(1) Users must be able to register an account
(2) Admin accounts can register user accounts

Since accounts will be a huge part of our system, we have to ensure that the process goes smoothly in the creation of an account. Some rules on account creation are as follows

(1) To create an account, a user must provide a username (email), password, date of birth, and location
    (a) Location includes city, state, and country)
(2) Administrator accounts will be able to create a user account

(a) The system will email the user with a first time login procedure explained later on

These rules will need constraints to properly create an account:

(1) An account creation will require the setup of security questions and answers

(2) A duplicate user of the same username cannot be created

(3) In order for an administrator to create a user account, they will need the username, date of birth, and location of the user.

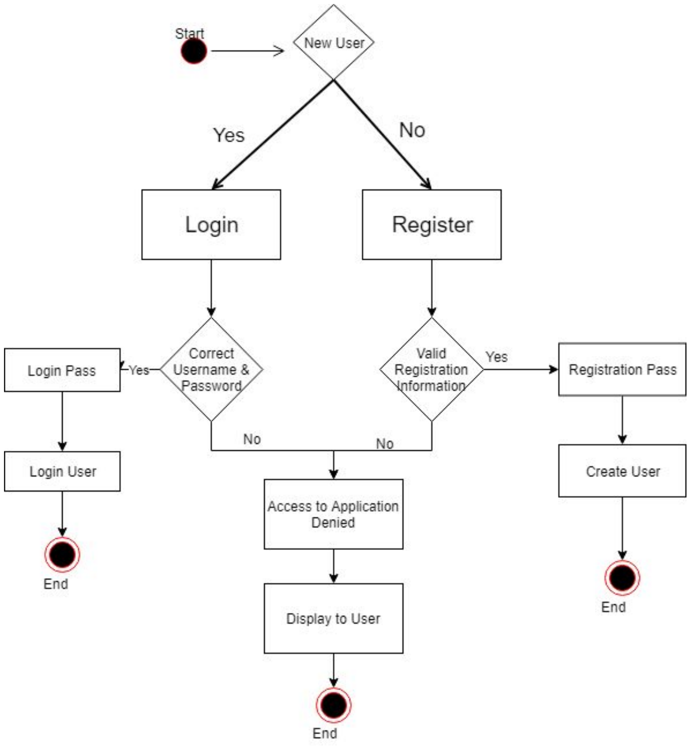
(a) A password will be randomly generated for the user account

(b) An email will be sent to the user with first time login procedures to do the following:

(i) Create a new password

(ii) Select 3 security questions and answers

(4) Date of birth must be older than 18 years from the day of account creation



Activation

Activation in our system includes the enabling and disabling of accounts by administrators. Some requirements around that feature include:

(1) Administrators must be able to enable and disable user accounts

(2) System Administrators must be able to enable and disable administrator accounts

These two rules aren't as simple as they seem though, some rules around requirements are as follows:

(1) Administrators will be able to toggle each account that they are allowed to enable or disable

(2) The system will notify disabled users upon login attempt

These rules show what the requirements do, but some constraints around the rules include:

(1) Active accounts cannot be activated and disabled accounts cannot be disabled

(2) Administrators cannot enable or disable other administrator accounts.

Activation allows the administrators to manage the users of the system. Disabling allows the reduction of abandoned accounts and also in case of the need for banning an account. Activation should only fail if the permissions rank of the target account is higher than the rank of the activators.

Deletion

Deletion within our system is similar to activation, except that users can delete their own accounts. The few requirements for deletion are:

(1) Users are able to delete their account at any time

(2) Administrators can delete any user account at any time except admin accounts

(3) System administrators can delete administrator accounts at any time

A main rule of deletion will be that whenever a user account is deleted, all PII associated with that account will be deleted as well. Similar to activation, fails should not occur if accounts can only be deleted by another with higher permissions than its.

Configuration

Configuration is the individual role settings for our system. Configuration has to do with User Access Control and similar to activation, account UAC can only be altered by a higher ranked account. Although business and customer accounts are the same level, they will have different access to the system. Through configuration, we are able to configure the different interactions both business and user accounts have with out system. For example, Business accounts will be configured to show a Business Analysis Dashboard, compared to User Accounts configuration of a Watchlist. The hierarchy configuration for all Accounts are: SysAdmin > Admin > Business / User Accounts. Only SysAdmin are able to delegate admin accounts, and modify the UAC of admin accounts.

Error Handling

Error handling on the client side of our system include handling all errors on the user's end. These errors will produce a readable message that will show further instruction to the user.

- Server request timeouts (server ran out of time for request), the server request was not valid, the server had an error, the inputted data is invalid, a user tries to access something outside of their permissions, and mainly, the errors would alert the system administrators for further actions

Any time a user come across an exception, a message will be presented to the user to inform them of the error which occured. The message will also recommend a way for the user to solve their issue. To measure how well our error handling is, anytime an error is handled it should not interfere or crash the system.

Error handling on the server side of our system include handling all errors which occur on the server side. Some of these errors include:

- Invalid requests (such as authentication expiring), Server errors which would be minimal with AWS servers, Unauthorized attempted access, and mainly, most errors would contact administrators for further actions on an error.

If an of the error must return to the user, a message will be presented to the user to inform them of the error which occured. Similar to how we measure how well our error handling is on the client side, anytime an error is handled on the server side, it should not interfere or crash the system with the exception of server or network shutdown. Fails in error handling would occur if the system fails to catch an error or an error is reported mistakenly.

Logging

Beside handling errors, every error will also be logged onto a database, along with other items. The logging will have rules for implementation. These rules are:

(1) Errors on both server and client side will be logged
(2) Specific functions must be logged
(3) Specific patterns of requests will determine an attack and will be logged

Additionally to the business rules, there are requirements we must meet to implement logging in a safe and efficient manner. The requirements are as follows:

(1) Notify a system administrator after 100 failed error log attempts
(2) Only system administrators are allowed to delete error logs
(3) To monitor denial of service (DOS) attacks, all server requests must be logged

All the logs will be stored in the database in a formatted manner. The contents of each log will include a timestamp of the error, the error name, the error location, which user caused the error, and what the user or system was trying to do at what point in the system. Logging will not only allow us to detect DOS attacks, but it will also allow us to find faults in our system. The logging system should be structurally sound, and fails should not occur when simply timestamping events.

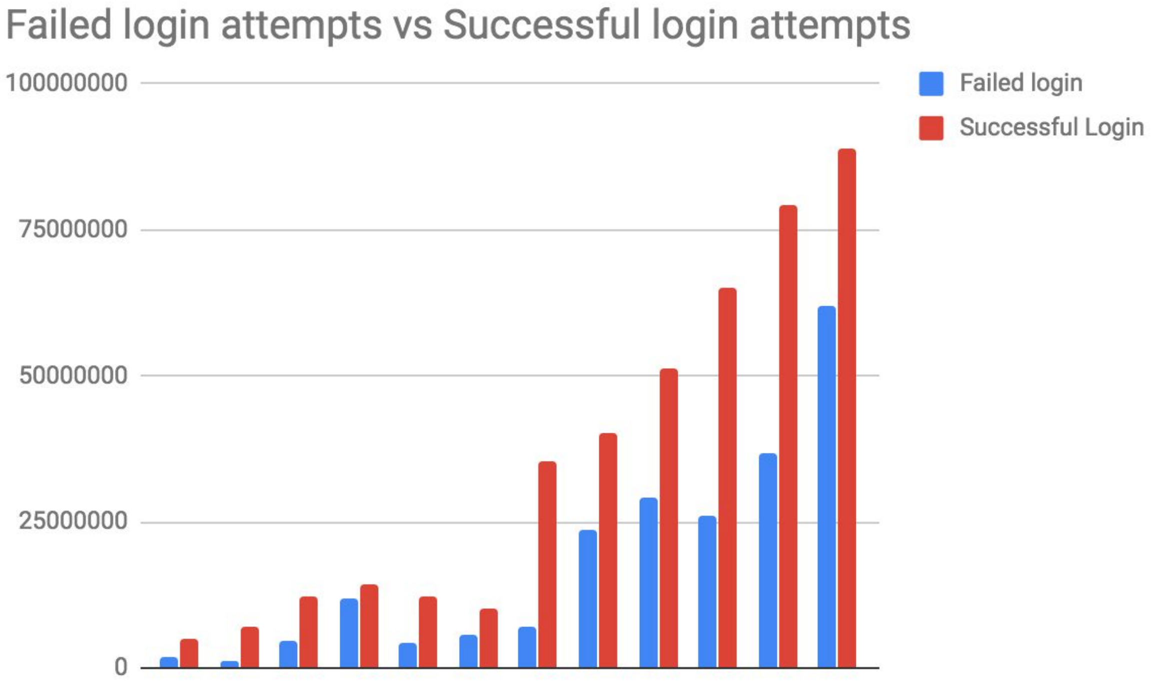
Log Archiving

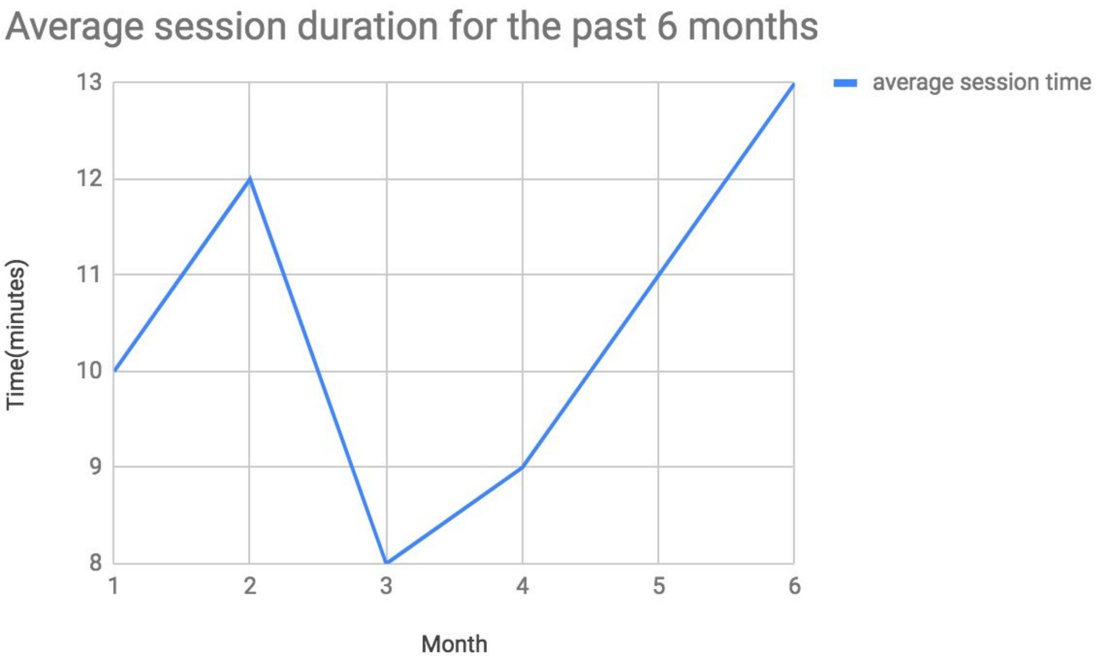
In order to avoid consuming all of our server space with logging, after a certain time period stored logs will be archived. Logs that are older than 1 month will be compressed and stored away while logs older than 2 years will also be compressed, archived, and then deleted off the system.

Given the amount of logs which will constantly be archived, there are bound to be some log archiving attempts which will fail. When a log archiving attempt fails, the system will retry to archive it after two hours. If a log fails to be archived more than three times, the system will notify a system administrator to take manual action. A log archive can fail if the criteria for backing up logs is not checked properly.

Usage Analysis Dashboard

In order to visualize the usage data for developers, we will represent logged data in bar and line charts. This will make it easier for developers to not only visualize the data but to find trends and analyze the data. Below are two examples of the charts we will be implementing.


Failed login attempts vs Successful login attempts


Average session duration for the past 6 months

Besides the two charts above, we will also be including 5 other charts which are as follows:

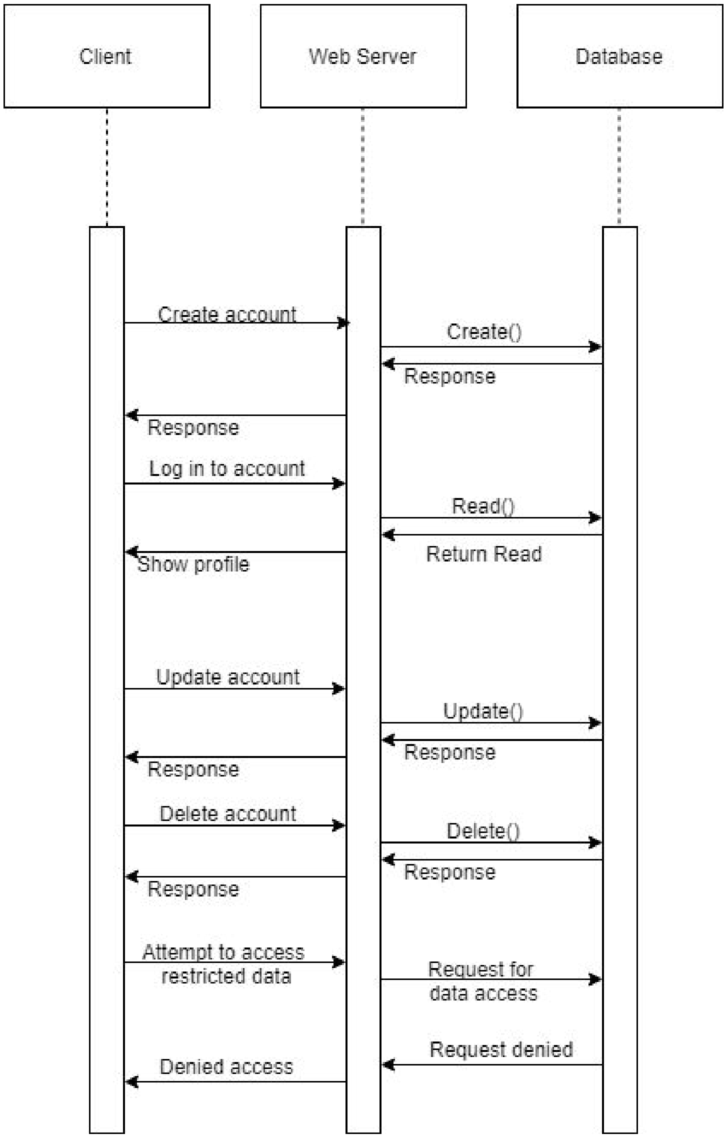
(1) A bar chart of the average logins per month vs total amount users.
(2) A bar chart of average session duration per month
(3) A bar chart of the five pages with the highest average time spent on them
(4) A bar chart of the five most used features in the system
(5) A line chart of the number of logged in users per month for the past six months

To measure how well our charts work we will be seeing how accurate the data is in the charts. The dashboard would only fail in the event telemetry is not logged properly.

Data Access Layer

The data access layer will handle all of the flow to and from our database. This subsystem will be able to create new data, read data, update data, and delete data. Given a specific user trying the access the data, the system will restrict the request accordingly according to their UAC. Invalid requests will return a simple 'Insufficient permissions' message which would result in a fail for data access.

Many rules around the data access layer prevent duplicate data, it will prevent data from overflowing, and will ensure the operations are atomic. The following sequence diagram shows the functionality of our data access layer.



User Manual

To make our system more user friendly we will be adding user manual documents for both developers and average users, as well as a frequently asked questions (FAQ) page. The developer documents will be meant to make it easier for developers to incorporate our system with theirs. The user manual documents are meant for regular users to learn how to use our system. The frequently asked questions page is meant to answer any frequently asked questions from regular users. Only the system administrator will be able to update the FAQ page. Access to any of the documents will not require authentication from the user.

Application Features

Search Engine

Our website will incorporate a Search Engine for our users. The function of our Search Engine will be to search the web for the lowest price of the desired item that the users has entered. Once these results have been found the results will be:

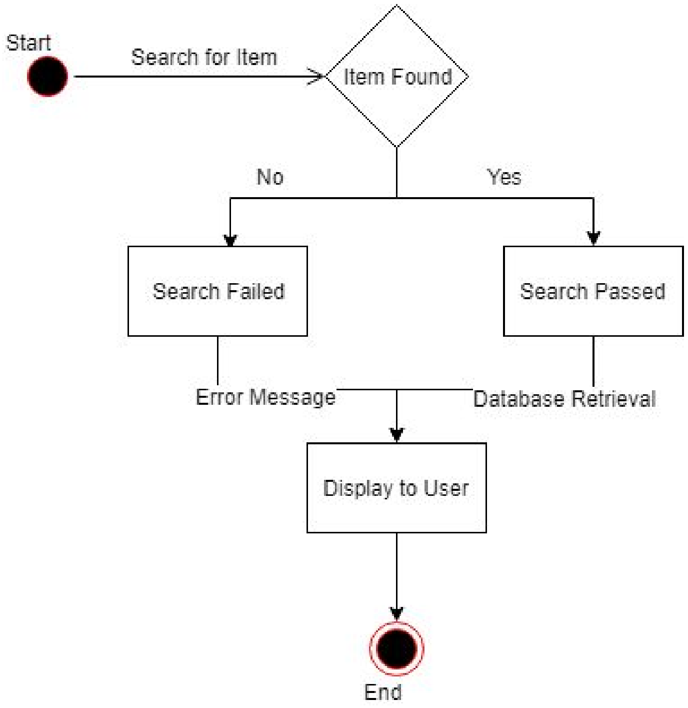
(1) Displayed to the user in a compact list view which will have a dynamic number of listings depending on the resolution

(2) The user will be provided with links to the item or directed to the item within our domain.

With displaying information to the users for the desired items, we must assure that the item we display to the user is accurate to what they have searched for. It is crucial to our system to display and search for the correct item. Coupled with displaying the correct item, it is also important to not show duplicate items unless there are more than one listing of the lowest priced item.

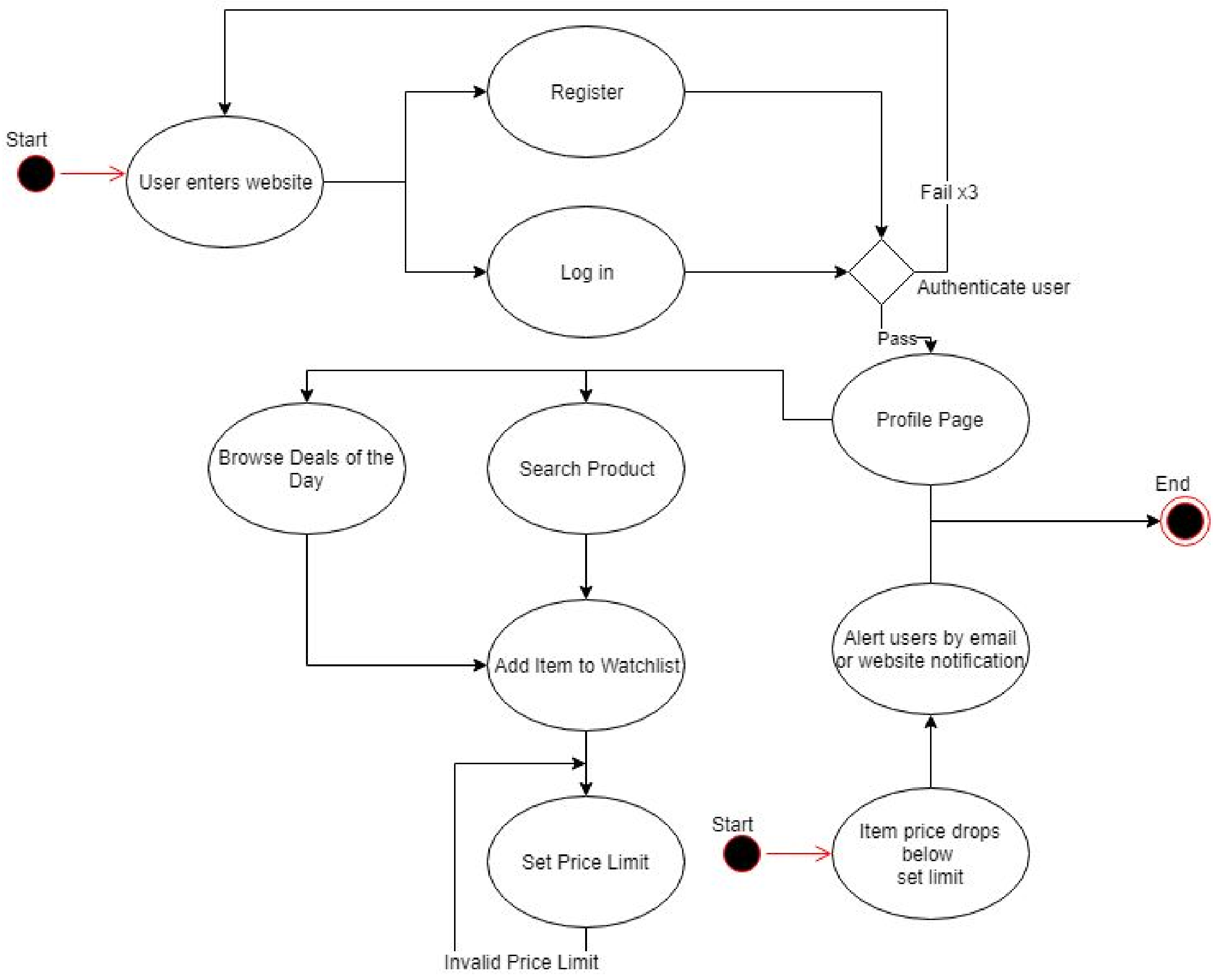
Based on these given constraints, displaying items within our scope to the users accurately is a huge priority to our system. In Addition, inadequately showing results would result in users seeking another site. For example, displaying the wrong item, false products, and a displaying the item after a few seconds delay would lead to users leaving our website for another service.

A scenario where search fails would be when no results are found. In this case, the system would return a page that indicates that there were no results found. Pass for searching would properly find and retrieve item information to display to the user.



Alerts

Providing low prices is the key point around our website. Should an item of your choice drop below a price you specified, the system will alert you either by email or as a website notification. The process of getting alerts is shown in the following activity diagram.



Some things we will fine tune in the background for alerts are as follows:

(1) We will ensure the user receives the alert as quickly as possible

(2) Our web crawler will compare major shopping websites such as Amazon, Walmart, Target, Ebay and Massdrop for an item to ensure a dropped price is not a false alert. This will be similar to trend watching. An item that decreases in price over time is more likely to be a legitimate drop.

 (a) We realize sales can produce a sudden drop and will research more into the specific algorithm at a future time.

Profiles

Users of our system will have two options regarding the types of profiles that can be created. The first type of profile is a regular user profile. This allows users basic access to our website and features. The other type of account is one for a Business. This allows the business to communicate directly with us to crowdsource items as well as allows them to sell product over our website. We require that users must be registered with our system to choose a membership type. Businesses must have an up-to-date business license to sell items. A profile of any type can only have one email associated to its account.

Some abilities that users have direct control of regarding their profiles include:

(1) Users can manage their account, i.e change password, update location, ect

(2) Users an edit their watchlists. They can add or remove items as well as share the list with other people.

The profile will be appropriately displayed to the user in a layout that adequately shows all the features associated with it. It is our duty to ensure that fake profiles that can sway analytics are properly dealt with. If a profile has been determined to be fake, it will be flagged for administrator review, then ultimately deleted. Profiles will only be created if registration criteria is met and that the authentication came back positive. A failed attempt at Profiles would be unsuccessful registration. Without a proper account, a profile cannot be made.

Deals of the Day

A feature of our website will include a Deals of the Day. These deals will be implemented given the following rules:

(1) Products must be within the top ten biggest price drops.

   (a) These deals will be calculated with the analysis dashboard.

(2) The list will be updated everyday in the morning at 00:00 PST

(a) An Item can be on the Deals of the Day more than one day.

To display this information to the user, we will have a feed that shows the Deals of the Day on our home page. It will show the item name, image of the item,time remaining, and the % of the discounted item. This feed will be updated dynamically and can be interacted with the user. For example the user can click on a certain Deal of the Day to be redirected to that item. Our future system will develop an algorithm to determine flash sales vs fake price drops and accordingly update our feed

One way for Deals of the Day to fail is no top deals were found. In this case, we would decrease the requirements for an item to become a featured deal and display the next tier of items in lieu of the regular deals.

Popularity Analytics

Given that our website will be able to log user data we can determine popular items and other useful data regarding user activity. Such requirements for popularity analytics includes:

(1) Items to be crowdsourced based on their popularity over a period of one month

(2) An account is required to be verified in order to judge popularity. In example a guest session will not be counted towards to popularity analytics.

Because of these requirements we must make sure to only consider data from users that are verified with our system. This information will be presented in a chart that can be accessed by admins and sysadmins. This data will be tied to our logging feature.

Privacy is a large concern so we will only be collecting data that is strictly required for Popularity Analytics, we will not be data mining everything. Users will also have the option to opt out of having their data tracked. We will also determine if the data we are collecting is organic, as in if a large amount of clicks are registered that does not look natural, we will disregard it. Unnatural clicks include large spikes in short periods, or a sudden climb from having no clicks. These inorganic trends would result in a fail for an items popularity. When this happens, we format the appropriate data to be sent to an system administrator for further review and action.

Small Business Promotions

Businesses that have created a Business Profile and have been verified, with their official business license, have the ability to post inventory they own to be posted and sold on our website. They will be able to sell extra inventory they normally would not be able to. Items will be listed on our website. They will remain on our website until they have no sales for a continuous 6 months. At that point, they will be notified of their customer traffic statistics. Further procedures on removing a business from our website will be determined at a future time.

Items from businesses must be:

(1) Displayed and show the amount of stock quantity left.
(2) Be searchable and showed in our results to the user if the user searched for an item that matched the criteria.
(3) Only verified Business Profiles can post items for sale.

It is important to also display the correct information that the business wants to post. We will first verify their items and then append them to our database to be shown throughout the website. A business would not be able to post to our website without going through the correct verification procedures.