2020

# WEB DEVELOPMENT PROPOSAL

PROPOSED TO:

STEVE GEORGE
edu@pagerange.com

PROPOSED BY:

THE INCREDIBLES TEAM
WDD 2020

**Proposal for E-Commerce Project**

Team Name: The Incredibles

Team members: Amandeep, Andrew, Erik, Jaspreet, Mayowa, Pournima, Shristi

University of Winnipeg Professional, Applied and Continuing Education (PACE)
Web Development Diploma (WDD)
November 30, 2020

**Description** **3**

**Project Details** **4**

**Proposed Design Solution** **6**

**Use Case** **9**

**Sitemaps** **10**

Front end sitemap 10

Back end sitemap 11

**Server** **12**

**Security** **13**

**Database** **15**

**Value Add** **16**

**ERD** **18**

**Our Team** **19**

# Description

The following is a proposal for an ecommerce website that sells smartphones to customers, primarily between the ages of 16 and 60, who reside in Canada. The user interface will appeal to a broad user group. The payment gateway will be optimized for shipping products to Canadian addresses, and international orders will not be permitted in this first iteration of the site. The primary interaction between a user and the website will be the multi-item shopping cart and payment gateway. Functionality will be discussed in greater depth in the section titled Project Details. The sitemaps contained herein show the hierarchy of all the website's pages.

This project will begin with the design process: creating a mockup of the key pages, then using these as a guide for coding and programming in later stages of the project. The preliminary designs are contained in the section of this report titled Proposed Design Solutions. Next, the developers will create dynamic pages based on the html templates that are populated by records stored in the database. The database configuration will be discussed in the section titled Database. The site will also include a user-friendly administrative panel which will enable an administrator to modify the content stored in the database. The admin panel will not be used by external users, therefore the design may not be synonymous with the user-facing pages. There will be two user groups aside from the admin user; Authenticated Users and Unauthenticated users. The features of the site that these three user groups will be able to access is explained in the Use Case section.

The website will be hosted on a Linux server that will be configured to maintain a high degree of security, while still enabling users to access the content. Server configurations and details related to security precautions are subsequently discussed in the sections titled Server and Security, respectively.

# Project Details

Here is a brief summary of some of the functional elements of the website.

- The home page will have three distinct navigation menus: main, utility and footer
- Product details will be stored in a MySQL database
- The Products page, “list view” will show a list of all records contained in the primary table of the database, and this page will also include a sidebar to allow users to sort the products by brand, operating system and colour
- On the Products page, pagination will enable the records from the database to be spread across several pages. The user will be able to click the numbered links to navigate these pages.
- The Products page will have a search bar, allowing the user to input keywords, and the site will return records from the database whose product name, description and category match these keywords
- Each record on the Products page will include a link that redirects to the detail view page
- The detail view page will output all attributes from the primary database table for a single record
- The detail view of a given product will show links to “similar items”, which are from the same category/brand
- The Contact page will contain a contact form that users can submit for general inquiries
- Users will be able to register by providing essential contact information: name, email address and password. Optionally, users will be able to store a mailing address in their profile, which can later be used as a shipping and/or billing address.
- Once registered, a user will be able to login and logout from the site

- The Utility navigation will display links for the Register and Login pages for Unauthenticated users, whereas Authenticated users will see Profile and Logout in the Utility navigation
- When a new user registers, the system will check to see whether or not their email address matches with any that are already contained in the database. They will only be allowed to register if there is no matching email address in the database. If there is a match, they will be redirected back to the registration page and a flash message will alert them that there is already an account with that email address.
- If a user is logged-in they will be able to add items to the shopping cart. If a user is not logged-in and they try to add an item to the shopping cart they will be redirected to the login page and a flash message will explain why they were redirected.
- Clicking the shopping cart icon will redirect an authenticated user to a page which lists the items in their shopping cart. If a user is not logged-in, clicking the shopping cart will redirect them to the login page and present them with a flash message to explain why they were redirected.
- From the Shopping Cart page, authenticated users will be able to click “Proceed to Payment”, which will redirect them to the payment gateway
- The first step of the payment gateway will be to request the user’s shipping address. They will be able to select an address that they have stored in their profile, or add a new address if they prefer. Then the system will ask the user if the billing address is the same as the shipping address. If the billing address is different from the shipping address, the system will prompt the user to select an address saved in their profile or to add a new address.
- The shipping address will enable the system to calculate taxes. Within Canada each province will have the appropriate tax rate applied. International orders will not be allowed in this iteration.

- Flash messages will provide descriptive and colour-coded messaging for users. Green denotes affirmative, red denotes negative. Typically these alerts will be used to explain that a user's request has either been approved or denied, or the reason why a user was redirected.

# Proposed Design Solution

The following screenshots were taken from the html templates that were designed to represent the home page, the list view page and the detail view page, respectively.

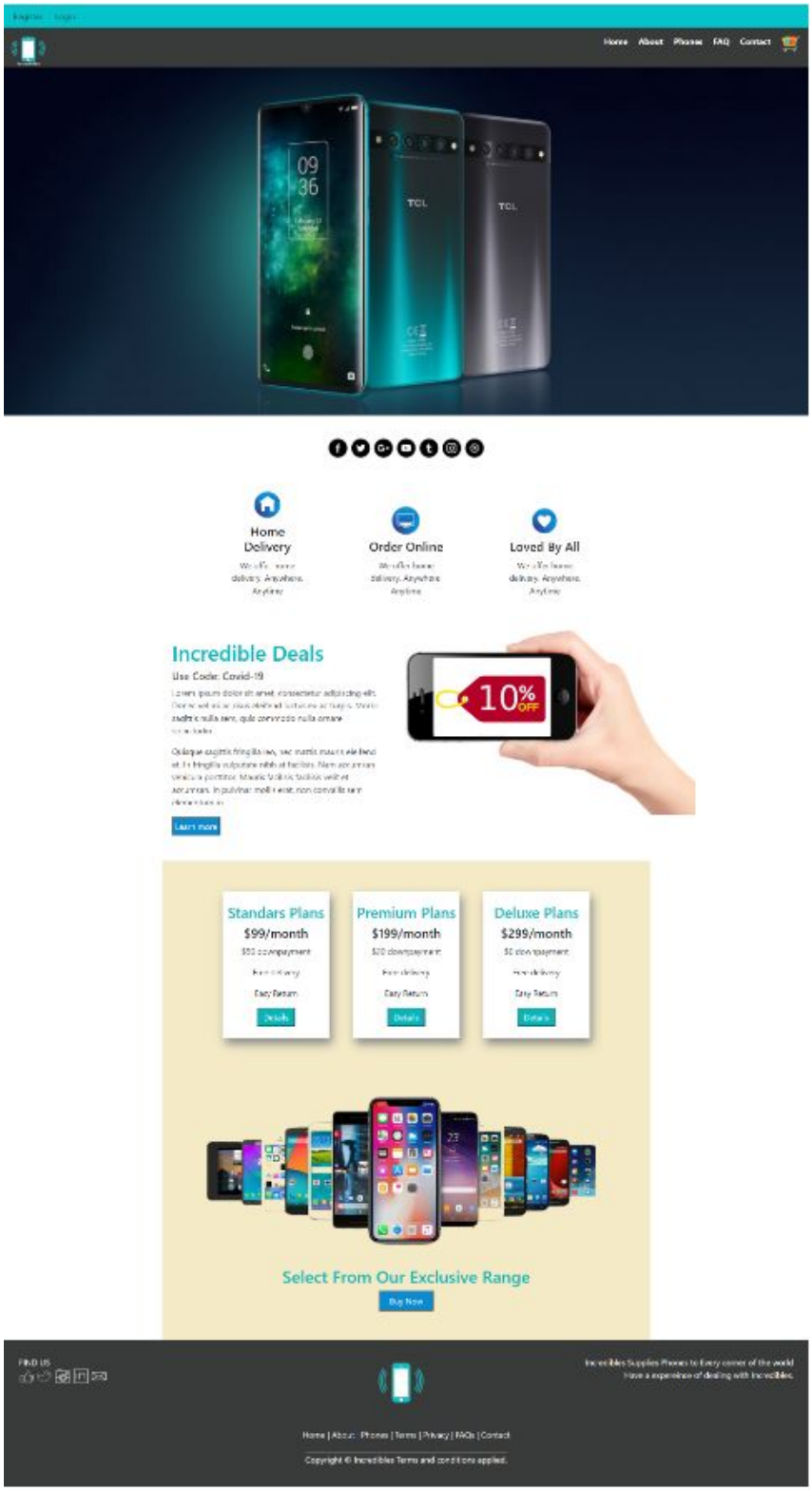



*Figure 1: a screenshot of the proposed home page*

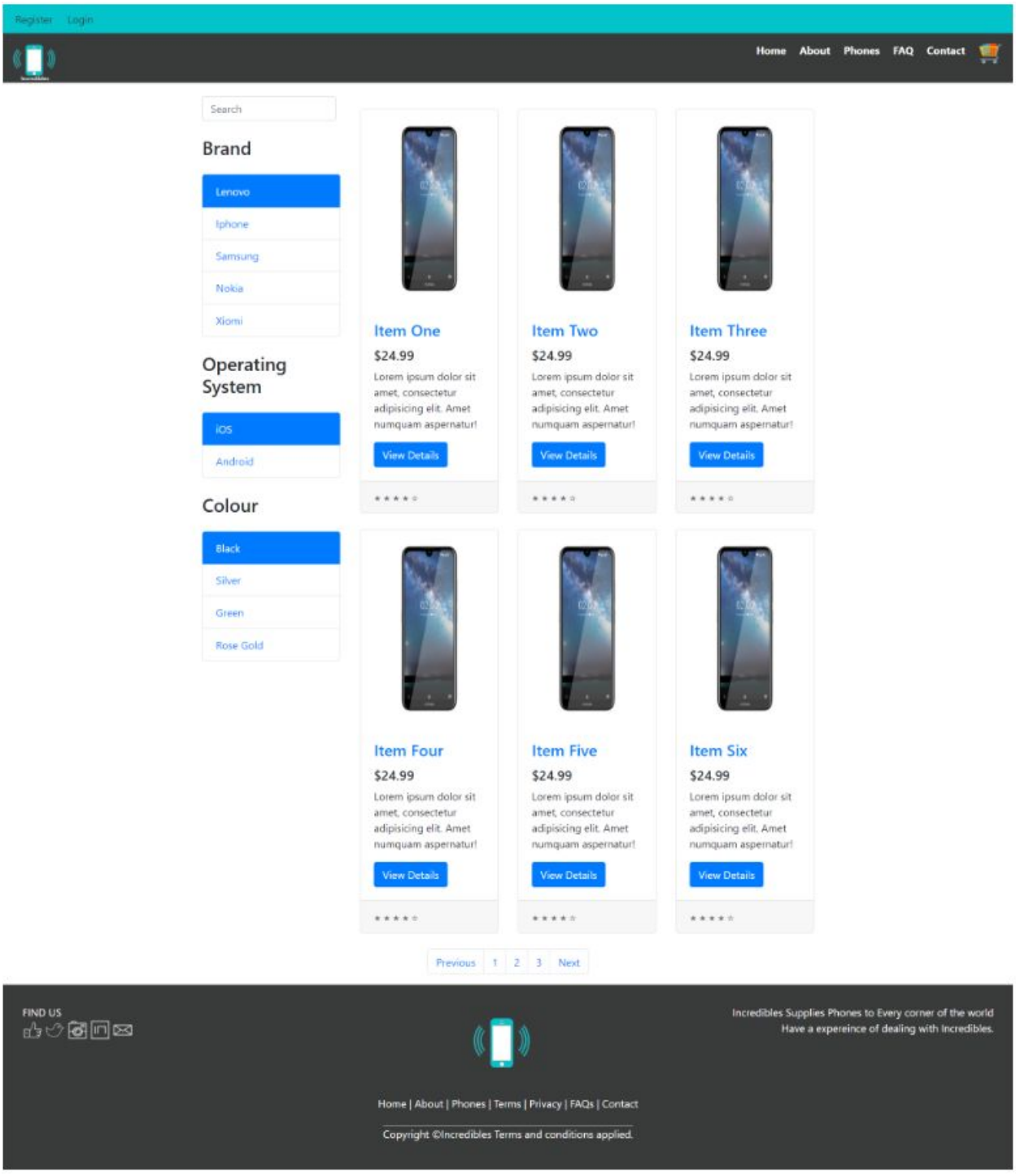



*Figure 2: a screenshot of the proposed Products page i.e. the "list view"*

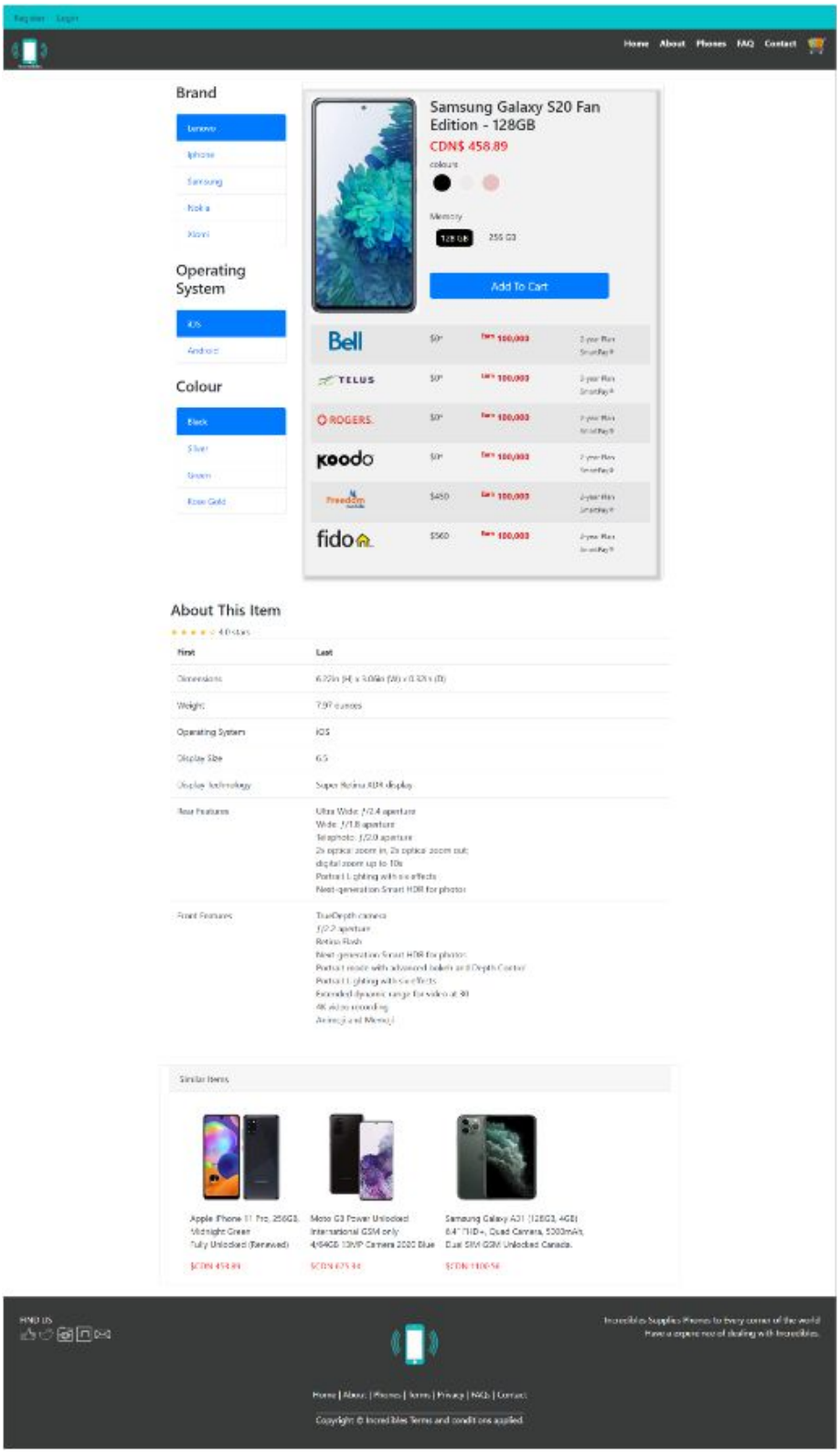



*Figure 3: a screenshot of the proposed product detail view page*

# Use Case

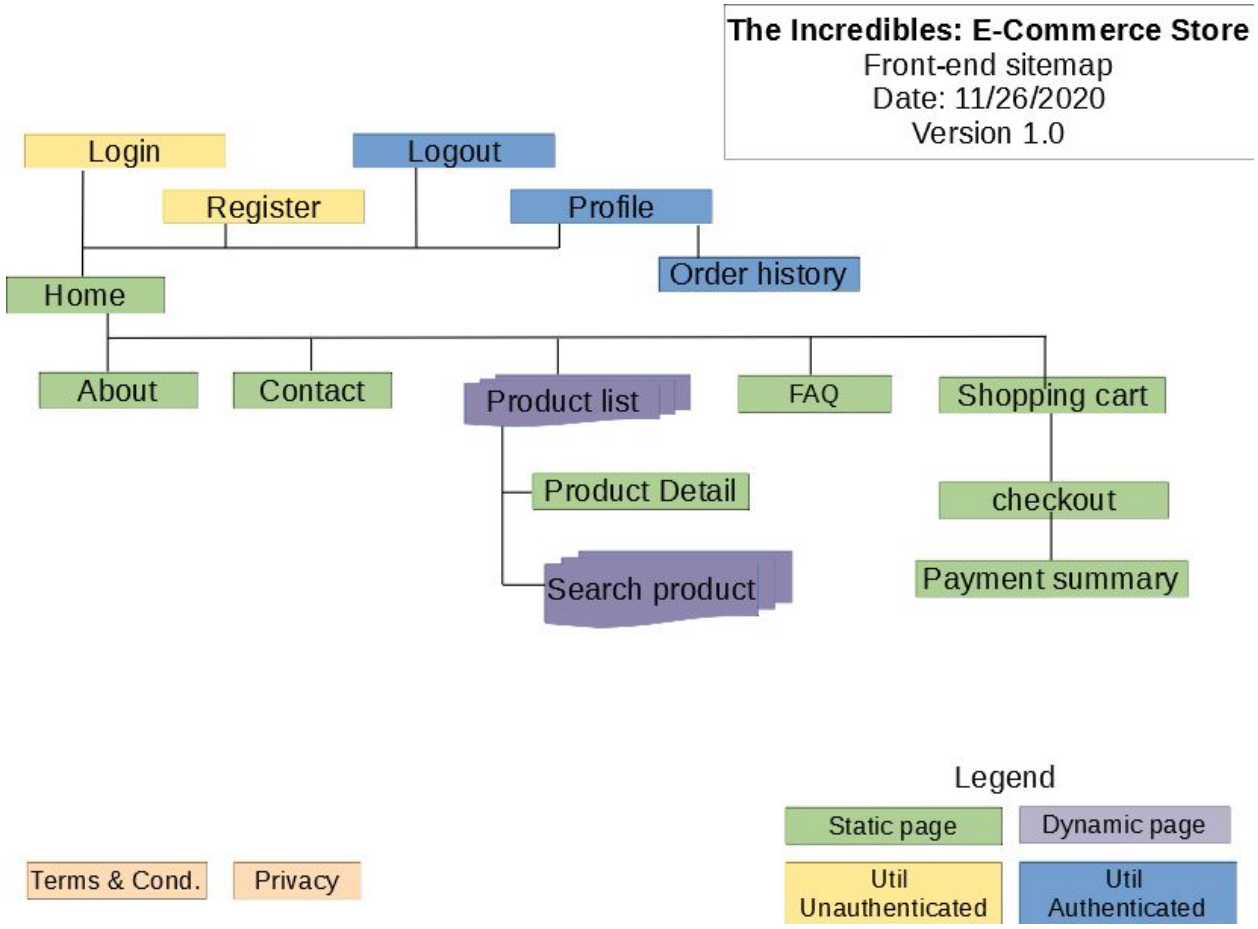
There will be three classifications of users on this site: Administrator (admin), Authenticated User (AU), and Unauthenticated User (UU).


The admin will have access to the back end components of the site, where they will be able to add/remove/edit items in all database tables: this includes products, users, product categories, orders, carriers, and taxation rates. The admin user will also be able to see a listing of the user activity log. Aggregate data on the content of the website and database tables will be displayed on the home page of the admin site. The admin user will use the same login form as a regular user, and once they have been authenticated they will see the links to the admin dashboard (which are never visible to other users.)

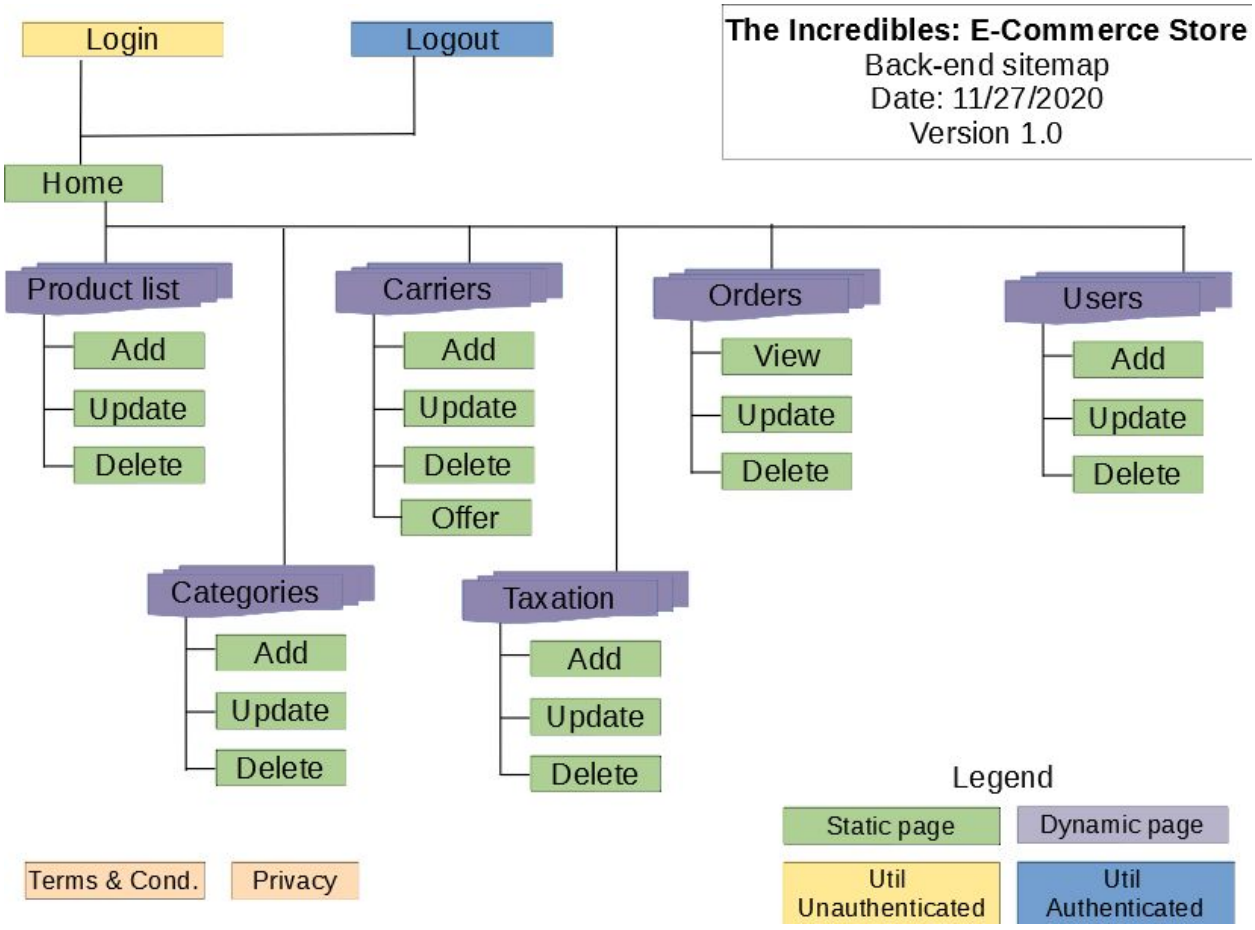
AU will essentially have all the same functionality as UU plus some additional features. Both UU and AU will be able to browse the products on the front end of the website, but only AU will be able to add items to their cart and proceed to the payment gateway to complete their purchase. AU will see links for “profile” and “logout”, whereas UU will see links for “register” and “login”. On the profile page, AU will be able to update their contact information.

# Sitemaps

## Front end sitemap



## Back end sitemap



# Server

The web site would be hosted on a remote server in Digital Ocean. We will be using the long term support version of Ubuntu Linux server which could ensure the stability and reliability. For database setup, MariaDB would be used because it would maintain the compatibility for data conversion. We will make use of the PHP Laravel 7 framework for development of the MVC design pattern.

The following information are the server configuration:

- OS: Ubuntu 20.04.1
- Database: MariaDB 10.3
- PHP version: 7.4.3
- Laravel version: 7.29.3
- IP: 134.122.35.19
- Domain name: incredibles.uwpace.ca

# Security

This section describes the security that was implemented on the server and that will be implemented in the project

**On the server**

1. Server Hardening and Security: Firewall is installed and configured to ensure network security and to monitor incoming and outgoing traffic. Rules are set up in the firewall configuration, which allows only certain network ports but block any unused or unneeded open ports.
2. SSL Certificate: Encrypt SSL Certificate called Certbot is installed to provide security for online communications. All communications between customers' browsers and the server will be encrypted to ensure safe transactions.

**On the Web App**

1. Password encryption: This Website is password encrypted which means when a user registers with the unique password and unique email, the password is being hashed using a strong one-way hashing algorithm, password_hash() and bcrypt algorithm, PASSWORD_DEFAULT before saving into the database. It is the best way to store a password which is personal to the user.
2. SQL Injection: As we want to protect our data from SQL Injection, we must take care of binding the values to the named parameter. This way the user information provided will be safe to interact with the database. For binding, refer to following steps:
    - Escaping the data.
    - Sanitize the data before it is inserted to DB – to protect our data from attacks.

3. User Authentication: Every user who attempts to login will be authenticated with valid email and password, which should match with values in the database.
4. Admin Authentication: A user has to be authenticated to access the admin portal. Those without the administrator's permission will be denied access with appropriate messages.
5. XSS Protection: Any pages that require user input are protected by escaping and filtering any harmful code to prevent cross-site scripting.
6. CSRF Protection: Hidden and unique values called CSRF tokens are embedded in every form. CSRF tokens prevent CSRF attacks because they validate if a request is from an authenticated user and block any other requests that do not have the same tokens, protecting the backend server.

# Database

The following are the list of all the database tables that will be created for the project:

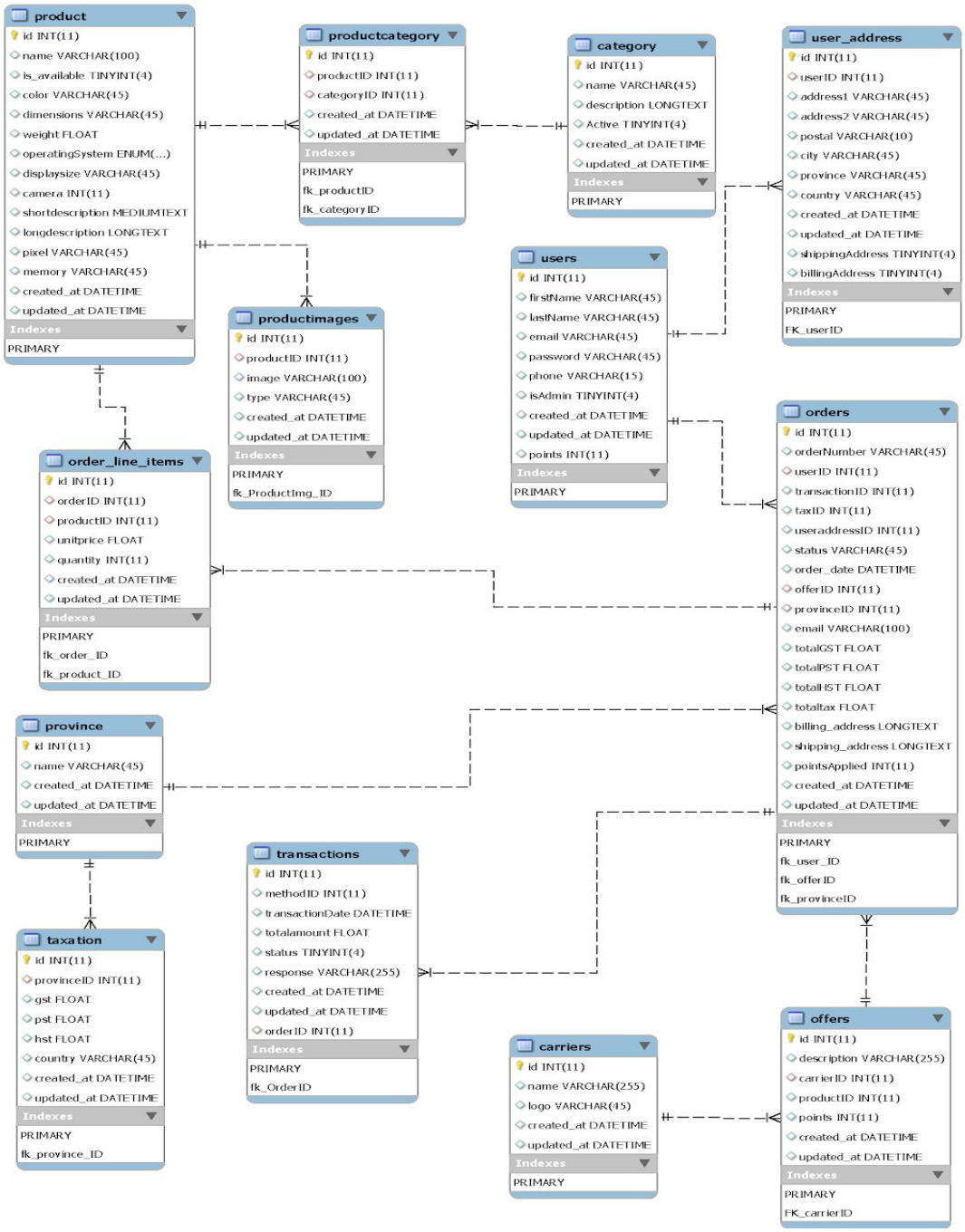

taxation
Contains list of gst and pst to be applied
offers
Contains list of current offers
invoice
Contains list of product invoices
payment_method
Contains list of product invoices
transactions
Contains list of all the transactions
carriers
Contains list of phone carriers

# Value Add

As a value add component, we are proposing to implement a points system where users can earn points with every purchase. This will be exclusively accessible to Authenticated Users, because Unauthenticated Users are not able to make a purchase, therefore they cannot accumulate points. These points can be exchanged for discounts on future purchases. The total points that a user has accrued will be displayed on their profile page. Points will be based on promotional offers, which are used as incentives for choosing to register the device purchased from this site with a subscription plan from one of the major telecommunications companies. Note that this is only optional, and users will be able to purchase the device without a subscription plan if that is their preference. Mobile devices purchased without a subscription plan will not be eligible for incentive points. Mobile devices purchased with a subscription plan from one of the major telecommunications companies will be eligible for incentive points. The numbers of points awarded to a particular device will be assigned based on the incentives given to our company from the telecommunications companies in exchange for our services in marketing their subscription plans.

# ERD

This is a graphical representation of all the tables contained within the database, including tables required for the value add feature that was discussed in the previous section.



# Our Team

- Amandeep - Front-end and back-end developer
- Andrew - Server administrator
- Erik - Project Manager
- Jaspreet - Front-end and back-end developer
- Mayowa - Git manager and back-end developer
- Pournima - Lead developer
- Shristi - Lead designer and front-end developer