

|  |  |
| --- | --- |
| Proposal for NINAsTEA Website Upgrade  May 27, 2021 | Abstract  Proposal of upgrading current static website to dynamic, database driven website for NINAsTEA company.  Xiaojing Shi  shi-x@webmail.uwinnipeg.ca  Flash Web Design  Steve George  [edu@pagerange.com](mailto:edu@pagerange.com)  [PHP Programming Capstone Project](https://nexus.uwinnipeg.ca/d2l/home/36617)  Web Development Program  University of Winnipeg, PACE |

Table of Contents

[Proposal for NINAsTEA Website Upgrade 2](#_Toc73023613)

[Introduction 2](#_Toc73023614)

[Features and Functions 2](#_Toc73023615)

[For customers 2](#_Toc73023616)

[For admin users 2](#_Toc73023617)

[Database 3](#_Toc73023618)

[Use Cases 4](#_Toc73023619)

[Unauthenticated users 4](#_Toc73023620)

[Authenticated users 4](#_Toc73023621)

[Admin users 4](#_Toc73023622)

[Security 4](#_Toc73023623)

[XSS protection 4](#_Toc73023624)

[CSRF protection 5](#_Toc73023625)

[SQL injection protection 5](#_Toc73023626)

[A Sample Form Submission 6](#_Toc73023627)

[Post 6](#_Toc73023628)

[Redirect 6](#_Toc73023629)

[Get 7](#_Toc73023630)

[Sitemap 8](#_Toc73023631)

[Front End Sitemap 8](#_Toc73023632)

[Back End Sitemap 9](#_Toc73023633)

[Physical Data Model 10](#_Toc73023634)

[Time Estimate 10](#_Toc73023635)

[Site Bible 11](#_Toc73023636)

Proposal for NINAsTEA Website Upgrade

# Introduction

NINAsTEA is a new local retailer based in Winnipeg, Manitoba selling teas. They are currently looking for a web development company to upgrade the current static website into a dynamic, database driven website in order to increase user experience and administrative management efficiency.

The main technology that will be used to make the upgrade are PHP and MySQL. First, we will create a database with MySQL with all data we need for the website organized and stored in different tables. Second, we will use PHP to convert all existing HTML pages into PHP pages with MVC(Model-View-Controller) pattern. This can better organized codes and make maintenance and changes easily. Third, with PHP and MySQL, we can get data from the database and dynamically render pages.

# Features and Functions

The overall goal is to upgrade the current website to a dynamic and database driven website. The upgraded website should have the following features:

## For customers

1. Search products. Customers can search products by keyword. Search bar is located on top of each page.
2. Sorted products. Customers can view products sorted by different categories.
3. Products list and detail information pages.
4. Make online orders. Customers can add products into shopping bag, edit quantities, view order subtotals, and make payment.
5. Add products to wish list. Customers can add products into wish list, as well as remove products from wish list. They can also save the list for later use.
6. Registration authentication. When a customer registers, the email provided will be verified and make sure it is unique in the database.
7. Log in and Log out authentication. Passwords entered will be encoded for website security.
8. After logging in, customers can view profile, wish lists, previous orders and make new orders.

## For admin users

1. Log in and Log out authentication.
2. After logging in, admin users can view products, customers, orders and logs.
3. On view products page, admin users can view, edit, and delete a current product, add a new product, and update database accordingly.
4. On view customers page, admin users can view all current customers.
5. On view orders page, admin users can view all previous orders.
6. On view logs page, admin users can view administration daily logs.

# Database

There are 5 tables in the database: customers table, teas table, orders table, order\_tea table, and log table; including following data type: integer, varchar, decimal, enum, boolean, text, char, date, datetime.

1. For customers table, data is collected mainly though registration process. We are collecting user's name, email, password, age, phone, address, city, province, postal code, country from registration form. With email and password, customers can log in and view profile, previous orders, wish list and make an online order. Beside, an unique customer id will be generated in database automatically. In order to distinguish a regular user and an admin user, privilege level is added with default value 0 for regular user and 1 for admin user.
2. For teas table, data is collected from NINAsTea company. This table is the primary table for the website. It includes all information of all products: product id, name, price, weight, type, caffeine, origin, expire date, organic, ingredients, description, SKU number, image. Customers can view product list and product details; sort products by caffeine level, tea type; search product with keyword; Admin users can add, view, edit and delete products from back end admin page.
3. For orders and order\_tea tables, data is collected from online order processes. After customers successfully make an online order, customer id, order date, subtotal, gst, pst and total amount will be stored in orders table with an auto-generated id. Tea ids, unite price, quantity and line price will be stored in order\_tea table. These two tables can interact with same order id. Orders table and customers table can interact with same customer id. Teas table and order\_tea table can interact with same tea id. In the end, we can use all these information to display a detailed order receipt.
4. For log table, data is collected when any user visit, view or interact with NINAsTea website. Every time an interaction occurred, it triggers the log function and file information of current date, request method, request uri, htto status of the request, information about the user's browser to the log table in database. Only admin users are able to view it after logging in.

# Use Cases

## Unauthenticated users

Icon

Description automatically generated

An unauthenticated user can visit all five main pages (home,tea,rewards,shipment,contact) through the main menu, he/she can view product list and detailed information; search for a certain product; add products into shopping bag and wish list; view the shopping bag; edit products quantities and remove products. But he/sha can not view the wish list or proceed to check out to place an order.

Icon

Description automatically generated

## Authenticated users

An unauthenticated user can register or log in to become an authenticated user. Once a customer registers or logs in successfully, he/she will land on profile page. From here, users can access to "My Orders" page to view all previous orders; "My Wish List" page to view products saved in the wish list. They can also remove products from wish list; add product to shopping bag directly from wish list; Proceed to check out and make an order.

Icon

Description automatically generated

## Admin users

Admin users can access the backend admin site. Once an admin user signs in successfully, he/she will land on the admin dashboard. From here, the admin user can view, add, edit, remove, and search products from "View Products" page; view all customers sorted by created time from the "View Customers" page; view all orders sorted by created time from the "View Orders" page; and view most recent 10 logs from the "View Logs" page.

# Security

## XSS protection

Cross site script injections are prevented by using PHP built-in htmlentities() function to sanitize data. This makes sure that all data get sanitized before getting used throughout the website.

## CSRF protection

Cross-site request forgery attacks are prevented by adding CSRF tokens to forms and session. Tokens are random and encoded values. When submitting, the token will be verified, and the form will be submitted only if the token matches the setting.

## SQL injection protection

SQL injections are prevented by using prepared statements. When interacting with database, to avoid the input be taken as part of SQL command, we bind parameter and thus force the input to be handled as parameters.

# A Sample Form Submission

## Post

When user click submit button, the registration form is submitted to the server through an HTTP POST request.

## Redirect

The server responds to the POST request by directing users to different locations. If the form does not pass the validation, the server redirects back to the registration form page with error messages; if the form pass the validation, server redirect to profile page with a flash message fading on the top of the page.

Graphical user interface

Description automatically generated

## Get

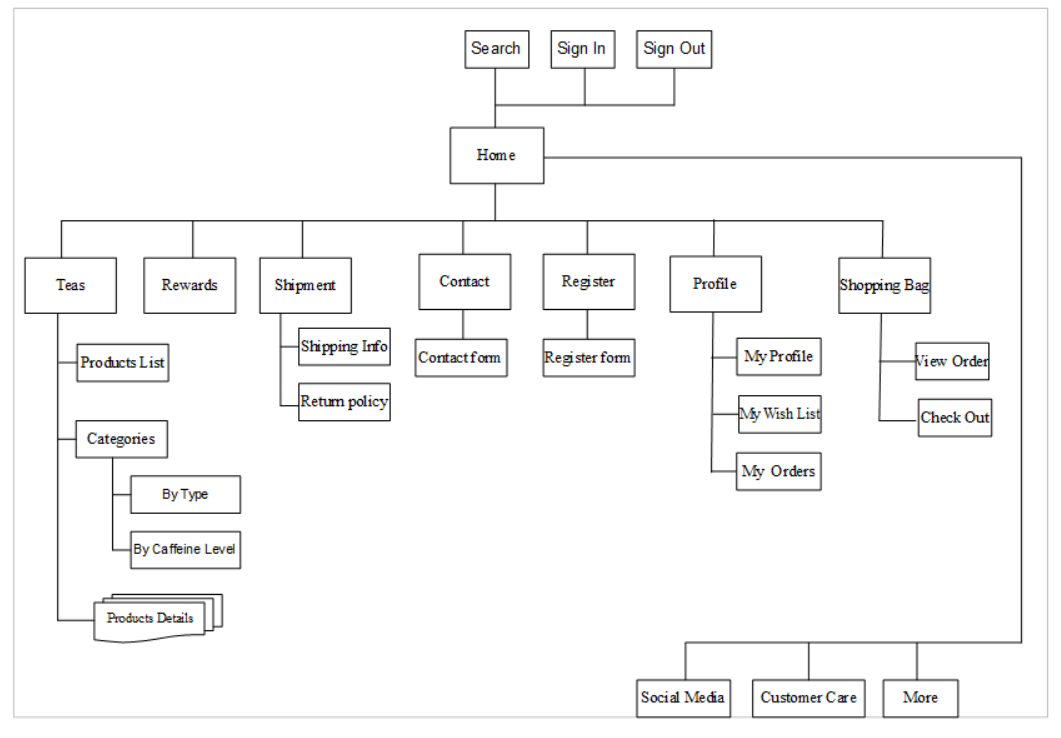
Once the server redirects users to the profile page, it retrieve data from the database and renders the profile page. And now users can see their profile information (not including password).

Graphical user interface, application

Description automatically generated

# Sitemap

## Front End Sitemap



## Back End Sitemap

**Diagram

Description automatically generated**

# Physical Data Model

Diagram

Description automatically generated

# Time Estimate

Phase 1: Database establishment

|  |  |
| --- | --- |
| Tasks | Estimated Time |
| Create five tables in the database and normalize to 3NF | 2 hours |
| Insert 20 records for the primary table and 5 records for other tables | 2 hours |

Phase 2: Front End HTML

|  |  |
| --- | --- |
| Tasks | Estimated Time |
| Website Redesign | 2 hours |
| Add new pages(static) to the current website | |
| Product detail view | 1 hour |
| Category view | 1 hour |
| Profile view | 1 hour |
| Register view | 2 hour |
| Sign in view | 1 hour |

Phase 3: Front End PHP Scripting

|  |  |
| --- | --- |
| Tasks | Estimated Time |
| Convert html files to php files | 2 hours |
| Create MVC folder structures | 2 hours |
| Components | |
| Config files | 1 hour |
| All controllers | 20 hours |
| All models | 4 hours |
| All views | 20 hours |
| All classes/validators | 4 hours |

Phase 4: Back End PHP Scripting

|  |  |
| --- | --- |
| Tasks | Estimated Time |
| Config files | 1 hour |
| All controllers | 20 hours |
| All models | 4 hours |
| All views | 20 hours |
| All classes | 1 hours |
| Validators | 1 hours |

Phase 5: Testing

Estimated time: 2 hours

# Site Bible

**Hosting/Cloud Provider**

**DigitalOcean**

**Server Type**

**Virtual private server (VPS)**

**PHP Version**

**PHP 7.4.15**

**IP of Server**

**143.110.218.200**

**URL of Project**

**http://capstone.wdd-nina-shi.xyz/**

**Admin User Login**

**Email:** [test@gmail.com](mailto:test@gmail.com)

**Password: MYP@SSWORD1**

**Regular User Login**

**Email:** [test2@gmail.com](mailto:test2@gmail.com)

**Password: MYP@SSWORD1**