60-334
Final Project Documentation
Winter 2014

Web Application Concept and Purpose Documentation

This is a fictional shopping website developed for users who visit typical websites for online shopping. Users are allowed to view and make purchase of items currently available on the website provided they are registered.

Apart from normal features of a shopping site, some value added features such as Credit Card validation, Emailing Customer have been excluded. As a team we took certain precautions to ensure that features such as Form validation, Shopping Cart, Adding/Deleting new Products/Categories were fully implemented with the use of Php ,MySQL,Html and Jquery. To make purchases possible we created our own currency called the ByteCoin. This was done in order to ensure the website is as close to what a user will get on a fully functional shopping site. More details on how various features were implemented will follow below.

Database Installation Instruction

The database is a MySQL database, administered through phpMyAdmin

Step 1)
Create a new phpMyAdmin account and take note of the database name, user name and password that you create.

Step 2)
Import the velrith_334.sql file into your database. This file contains all the SQL tables used on the website and some pre-populated data

Step 3)
Open lib.php. Towards the top there is a function called query_db. In this function you will find 4 variables:

```
$dbname = " "; //database name
$user = " "; //user name
$pass = " "; //password
$host = "localhost"; //keep host has localhost
```

Enter your created database name, user name, and password. Keep the host as “localhost”. The database should know be linked to the website files.

Web Application Installation Instruction

Individual images from the “productImages” folder should be placed in the private_html folder such as “.../private_html/logo.svg” or “.../private_html/arctic.jpg”.
All other pages/documents should be placed in the public_html folder such as “.../public_html/index.php” or “.../public_html/stylesheet.css”.

Web Application User Walk-through

Welcome to “The Adventure Store”. You can find a live example of the website at http://334.velrith.myweb.cs.uwindsor.ca/index.php. To begin the walkthrough we’ll first explain the main index.php screen that you are looking at.

index.php

You’ll see the title of the website at the top. Clicking on the website title will always bring you back to index.php. On the left you’ll see the login area and below that you’ll see the product categories “The Adventure Store” offers.

Scroll down towards the bottom of the page and you’ll see the footer area. Here you’ll see a link to the Contact Us page, the Careers page, and the terms and conditions. At the very bottom you’ll see our **SVG logo.**

terms.php

This page lists our terms and conditions of usage of our website.

contact.php

Click on the “Contact Us” page. On the **“Contact Us**” page you’ll see a form you can fill out to contact an administrative user. You can fill out the form and send a message if you’d like.

careers.php

Scroll down towards the bottom footer of the page and you’ll see a link called “Careers”. Click on this link. This page is a **XML/XSLT** formatted page, where you can see open positions at “The Adventure Store”.

list.php

Now lets check out some products in the store. Towards the left you’ll see the menu area with some links to product categories. Click on the “Weapons” category. Click on the various categories to check out the other products in the store.

product.php

Now from the list of products, select a product you’re interested in. Here you can see the product in greater detail. Note that the product picture is storied and retrieved from the **private_html** directory. Also note that there is no option to add the product to your shopping cart because you need to be logged in as a user to do so.

adminpage.php

To log into the administrative portion of the website, log into the website using the user name “admin@admin.ca” and the password “admin”. You will now see the admin section of the page. You can add new products to the inventory, delete an inventory item and edit the price of a product. You can create/edit products if you would like. Now log out of the admin account by clicking the “Log out” link in the menu area.

register.php

Let’s create an account now. In the left menu area, just to the right of the “Login” button, you’ll see a “Sign Up” link. Click on this link to be directed to the account sign up page. Note that **AJAX** is used in the “Confirm Password” field to ensure that the passwords match. It is used in the “E-mail” field to ensure a valid email address is entered. And it’s used in the “Phone Number” field to ensure a valid phone number is entered. Fill out the form and click “Submit” to create your account. Your newly created account will be endowed with 300 ByteCoins to spend in “The Adventure Store”. You’ll now be automatically redirected to the “My Account” page.

myaccount.php

In the “My Account” section you can view your ByteCoin balance along with your order history.

mysettings.php

On the left menu select “My Settings” to edit your personal information.

Make a purchase

Now let’s buy some stuff!! Go ahead and add some products to your cart. Note that on the product page that selecting “Add To Shopping Cart” and “View Shopping Cart” do two very different things. “Add To Shopping Cart” adds the product you are viewing to the shopping cart. While “View Shopping Cart” does not modify your shopping cart.

cart.php

Once you are happy with the items in your shopping cart, you can now check out. Note that you can remove individual items from the cart by selecting the “Remove” link under the product name. You can completely empty your cart by selecting the “Clear Cart” button in the total area.

You can adjust the quantity of the product you are buying by editing the quantity field for each product and selecting the corresponding “Update” button to update your total. Note that if you do not have enough ByteCoins in your account to make the purchase an appropriate message will be displayed.

Other non-admin login usernames/passwords

email1@email.com	→	email1password
email2@other.co	→	email2password
a@b	→	c

Security Features

All pages that are receiving data in the form of a POST command, a GET command, are checked for the right number of arguments and that their names match what they are expecting. Upon satisfying that criteria, the information gets parsed to get rid of any possible html injection attacks by converting certain symbols that may represent metadata (<, >, ‘, “, &) to a different ‘safer’ representation using the function htmlspecialchars(). Pages that require one or more database queries would also have their information parsed by the same function before usage. A few files that use this extensively include “update_inventory.php”, “cart.php”, “list.php”, “myaccount.php”, “mysettings.php”, and “lib.php”. Other files that use this less include “adminpage.php”, “contact.php”, “getimage.php”, “InsertNewUser.php”, and “logout.php”.

Besides preventing html-injection attacks, databases can also be prone to SQL-injection attacks. These can be prevented by using SQL prepared statements. All queries to the database go through the function “query_db()” that is in the “lib.php” file. This function takes as input the prepared statement and an array of the substituted named variables, and it prepares the statement correctly before querying the database and returning a PDO object with the query results.

Moreover, users’ passwords are hashed using MD5 before storing them in the database. The password from login attempts are hashed first (without trimming), before comparing against the hash code stored.

Furthermore, certain pages such as “myaccount.php” are only available/functional for users once they are logged in, and certain pages such as “adminpage.php” are only available/functional to admins.