Logo, company name

Description automatically generated

**WEB APPLICATIONS & DATABASES**

**C S T 2 1 2 0**

*Coursework 2*

*Final Submission*

Lab Tutor: Parvesh Seeburrun

Submission Date: 21/02/2023

Student Name/s:

Bibi Shawanah Ally

Kenechukwu Chukwudumebi Ajufo

Heman Kumar Ramrecha Bhagloo

Student Number/s:

M00851117

M00804152

M00788767

Table of Contents

[Table of Figures 3](#_Toc127909284)

[Introduction 4](#_Toc127909285)

[The Websites 4](#_Toc127909286)

[E-Commerce 4](#_Toc127909287)

[Home page 4](#_Toc127909288)

[About page 5](#_Toc127909289)

[Products page 6](#_Toc127909290)

[Contact page 7](#_Toc127909291)

[Cart page 7](#_Toc127909292)

[Customer dashboard 8](#_Toc127909293)

[Searched results page 10](#_Toc127909294)

[Login page 10](#_Toc127909295)

[Signup page 12](#_Toc127909296)

[CMS (Customer Management System) 14](#_Toc127909297)

[Login page 14](#_Toc127909298)

[Home page 16](#_Toc127909299)

[Product Page 16](#_Toc127909300)

[Security, Privacy and Legal Issues 18](#_Toc127909301)

[Security issues 19](#_Toc127909302)

[Privacy issues 19](#_Toc127909303)

[Legal issues 19](#_Toc127909304)

[How were these issues addressed on the website? 19](#_Toc127909305)

[How can unresolved issues be addressed in the future? 20](#_Toc127909306)

[References 21](#_Toc127909307)

# Table of Figures

[Figure 1: E-commerce Home page 4](#_Toc127913410)

[Figure 2: E-commerce About page 5](#_Toc127913411)

[Figure 3: E-commerce Products page 6](#_Toc127913412)

[Figure 4: E-commerce Contact page 7](#_Toc127913413)

[Figure 5: Message displayed when product added to cart 7](#_Toc127913414)

[Figure 6: E-commerce Cart page 8](#_Toc127913415)

[Figure 7:Confirmation message upon successful purchase 8](#_Toc127913416)

[Figure 8: E-commerce Customer dashboard 9](#_Toc127913417)

[Figure 9:E-commerce Past orders 9](#_Toc127913418)

[Figure 10: E-commerce searched results 10](#_Toc127913419)

[Figure 11:E-commerce Login page 11](#_Toc127913420)

[Figure 12: Login error messages 11](#_Toc127913421)

[Figure 13:Login successful login message 11](#_Toc127913422)

[Figure 14: E-commerce Signup page 12](#_Toc127913423)

[Figure 15: Sign up input validations 12](#_Toc127913424)

[Figure 16:Sign up error messages 13](#_Toc127913425)

[Figure 17:Sign up successful registration message 13](#_Toc127913426)

[Figure 18: CMS Login page 15](#_Toc127913427)

[Figure 19: CMS Home page 16](#_Toc127913428)

[Figure 20:CMS Product page 17](#_Toc127913429)

[Figure 21:Add product 17](#_Toc127913430)

[Figure 22:Edit product 18](#_Toc127913431)

[Figure 23:Delete product 18](#_Toc127913432)

[Figure 24:Password validation 19](#_Toc127913433)

[Figure 25; Parameterized query and Data sanitization 20](#_Toc127913434)

[Figure 26: Error handling 20](#_Toc127913435)

[Figure 27: AJAX query 20](#_Toc127913436)

# Introduction

The report includes screenshots of different pages from the e-commerce website and content management system (CMS), along with functional information for each page.

The e-commerce website includes home, about, products, contact, customer dashboard, search results, login, signup, and cart pages, while the CMS includes home and login pages.

The report also covers security, privacy, and legal concerns that affect the website and suggests solutions to address them.

# The Websites

## E-Commerce

‘Linterdit’ is an e-commerce website based on skincare and was created to provide customers with an enjoyable and secure purchasing experience, with a simple and user-friendly interface. The website consists of key functionalities like product listings, product recommendations, shopping cart, checkout, registration and login procedures, customer dashboard and search query.

### Home page

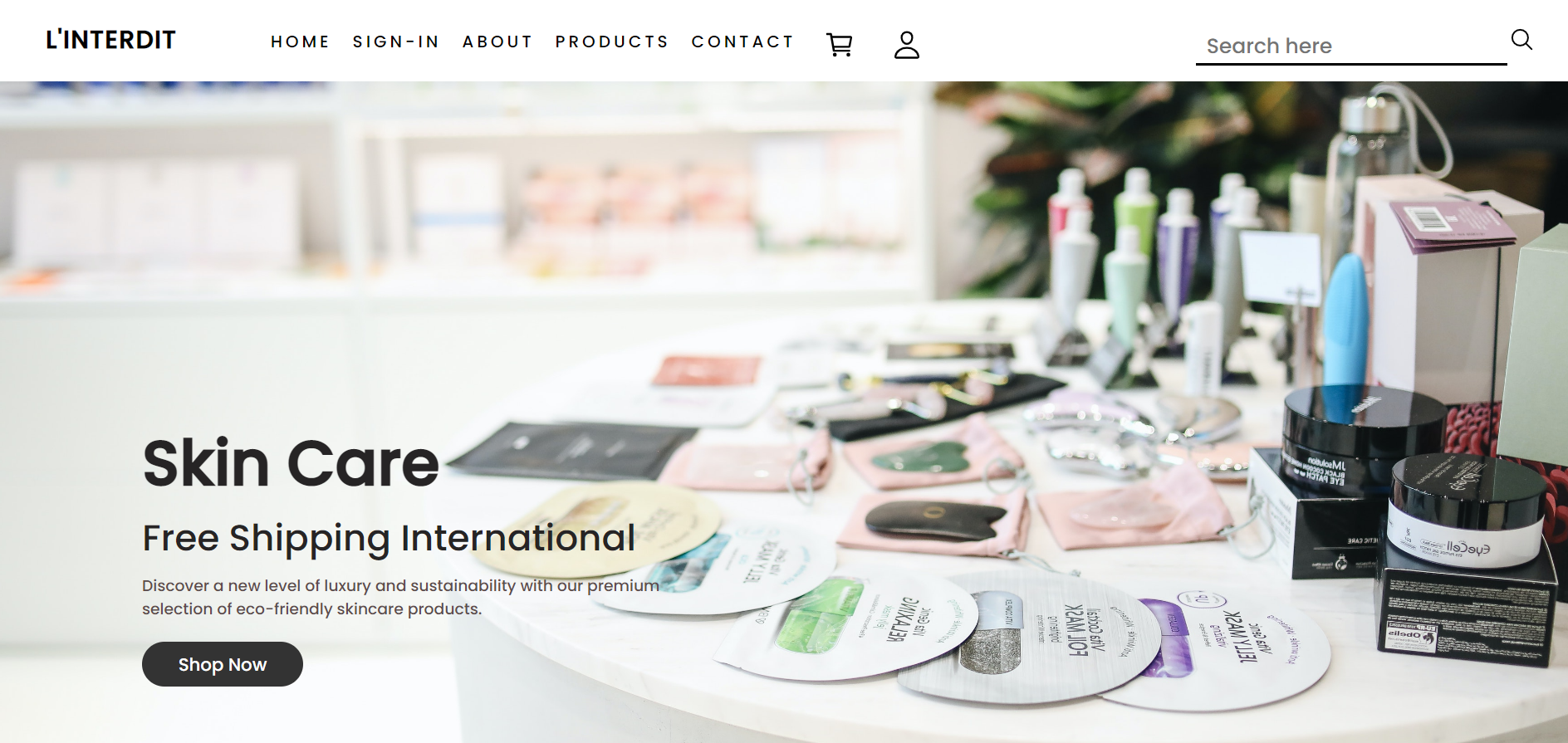


Figure 1: E-commerce Home page

Once the customer is logged in, they can begin their shopping experience. They have two options for finding the products they need: they can either use the search box at the top of the page and enter relevant keywords, or they can navigate to the "Products" link in the navigation bar. Additionally, the customer can type in the name of a specific product in the search box to find it more easily.

### About page

Graphical user interface, text, application, email

Description automatically generated

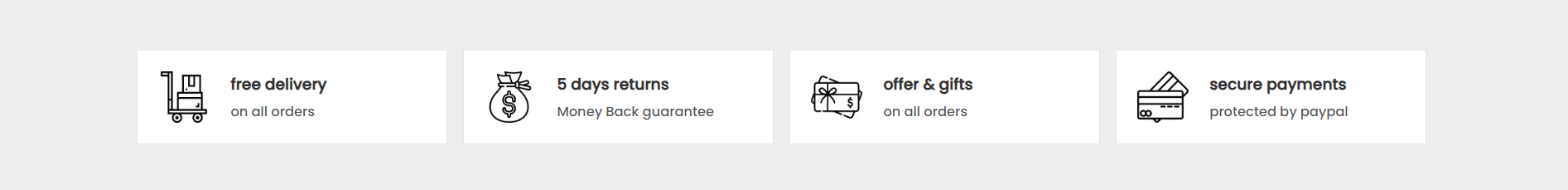
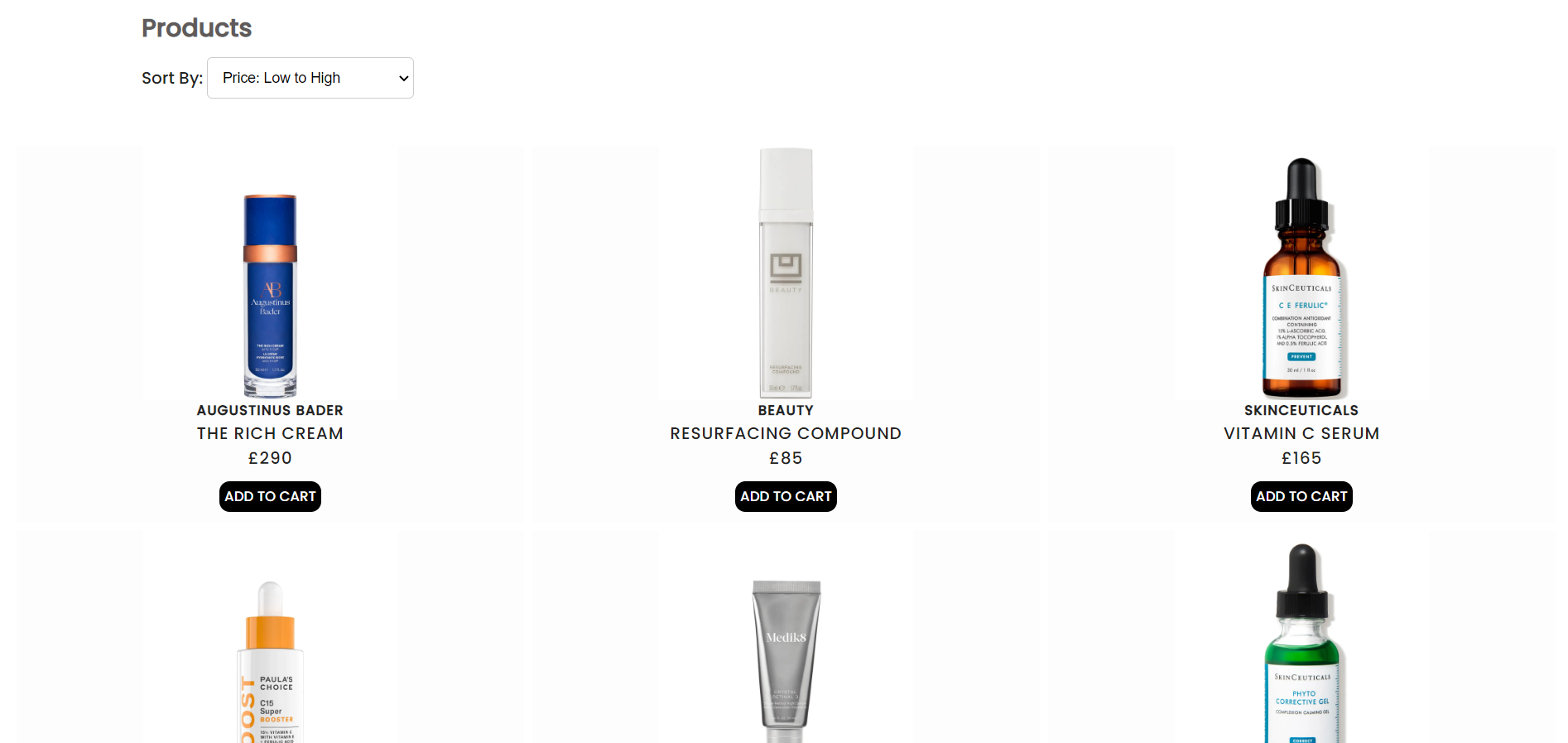


Figure 2: E-commerce About page

The About page is a crucial part of any e-commerce website as it provides users with the necessary information to make informed decisions about the products and services offered. It contains important details such as policies, delivery information, and services offered. The page aims to provide visitors with an overview of the website's key information.

### Products page



Graphical user interface, application

Description automatically generated

Graphical user interface

Description automatically generated with medium confidence

Figure 3: E-commerce Products page

On the products page, customers can see all the products that are currently available. To add a product to their cart, they simply need to click on the "Add to Cart" button and can continue browsing other items. Once the customer clicks on "Add to Cart," the selected product is then added to their cart page. The latter is only possible if the user is logged in.

### Contact page

Graphical user interface, application

Description automatically generated



Figure 4: E-commerce Contact page

To provide customers with the best possible customer service, the website has a "contact us" feature located at the bottom of the page. This feature includes the shop's contact information, such as a customer care phone number, email address, and physical address. Additionally, the website's footer includes links to specific pages for quick navigations.

### Cart page

Graphical user interface, text, application

Description automatically generated

Figure 5: Message displayed when product added to cart

Table

Description automatically generated

Figure 6: E-commerce Cart page

Graphical user interface, application

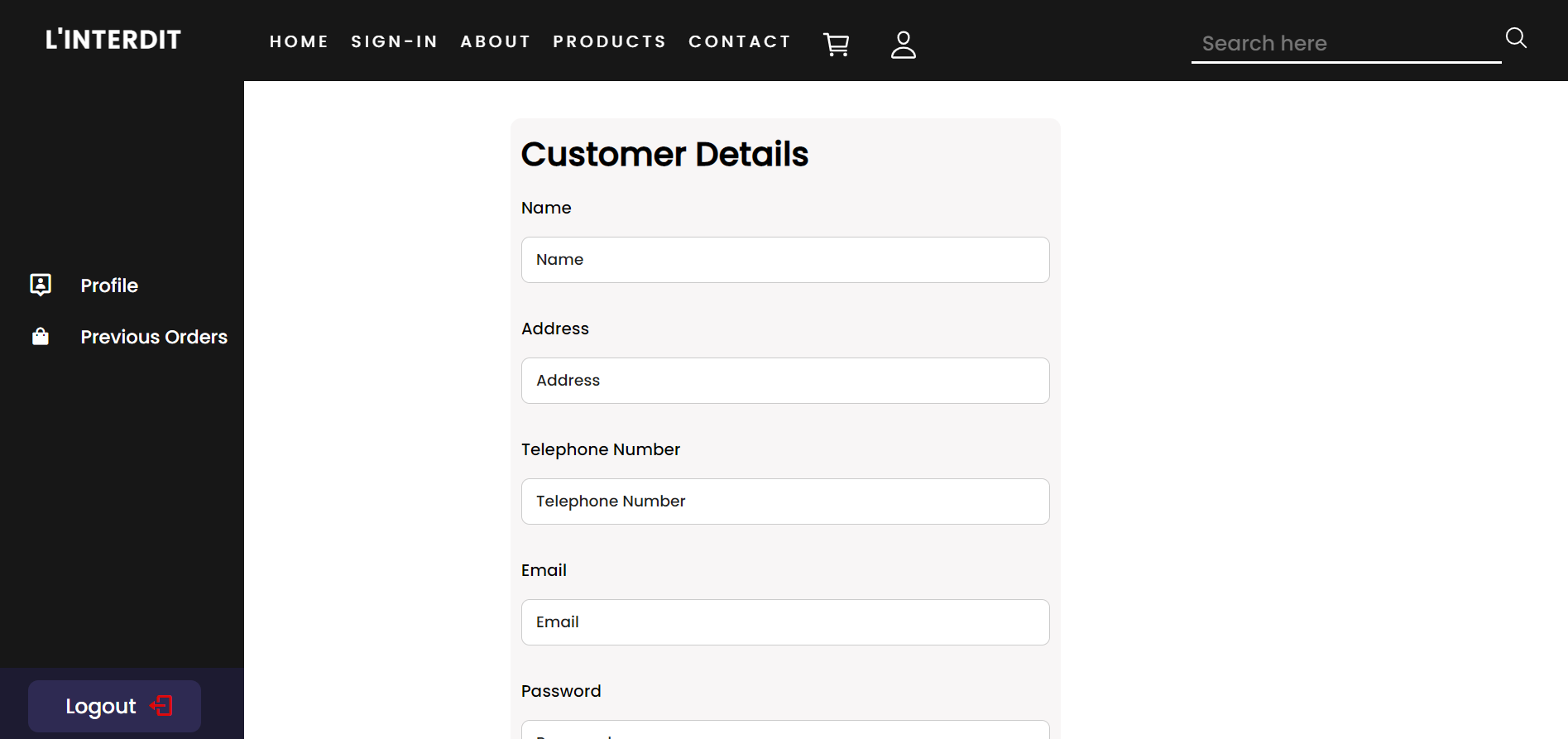
Description automatically generated

Figure 7:Confirmation message upon successful purchase

The Cart page is where customers can see all the products they have added to their shopping cart,along with the total price.

Once the customer is satisfied with their selections, they can click on “checkout” button and a confirmation message will be displayed. The user’s basket is then emptied.

### Customer dashboard



Graphical user interface, application

Description automatically generated

Figure 8: E-commerce Customer dashboard

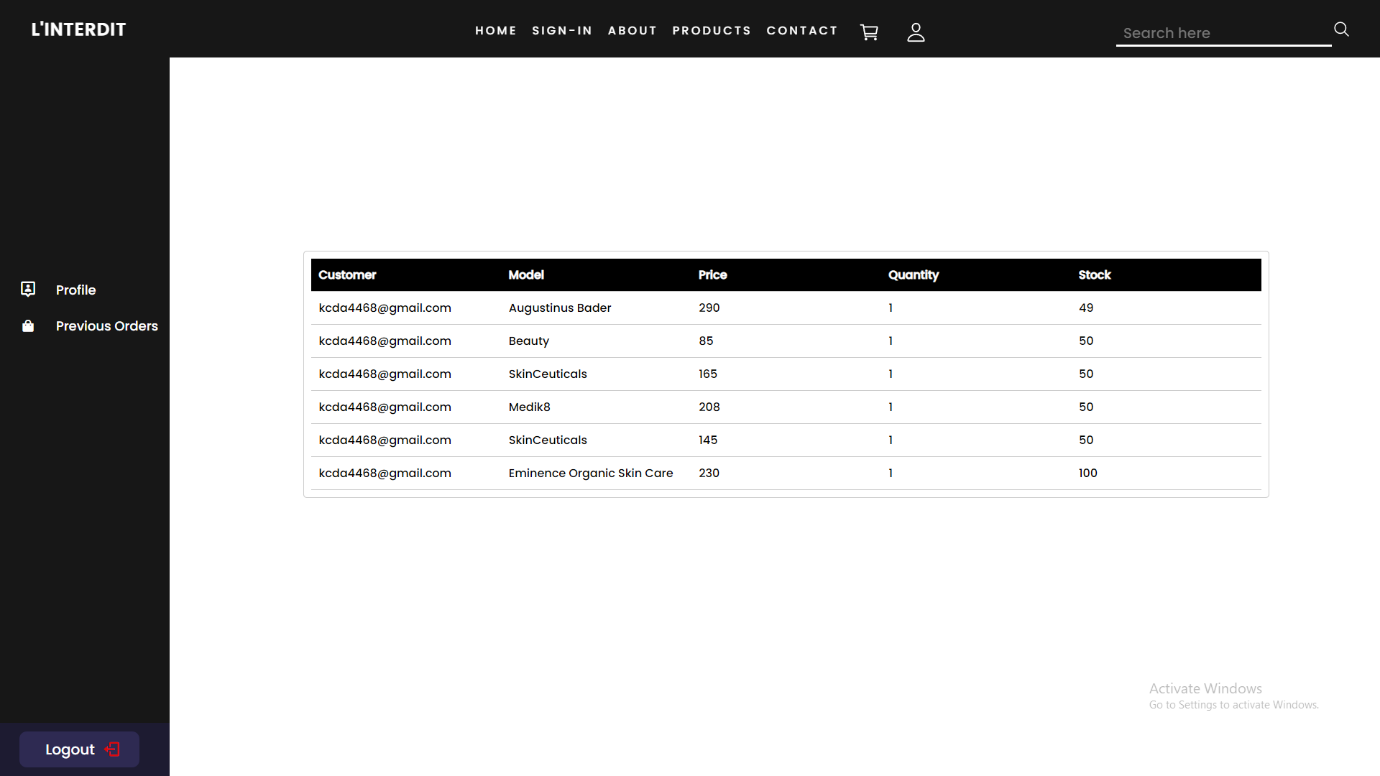


Figure 9:E-commerce Past orders

The customer dashboard has options like viewing and editing customer details as well as prior order history.

The latter can only be used if the user is signed in.

The customer can access and modify his information in the "profile" section. By pressing the "edit" button, the information about the currently logged-in user is displayed. The user only needs to alter the data in the input fields and click "save" to make changes.

A list of the customer's prior orders, including the item ordered and the price, are shown in the "previous order" section.

### Searched results page

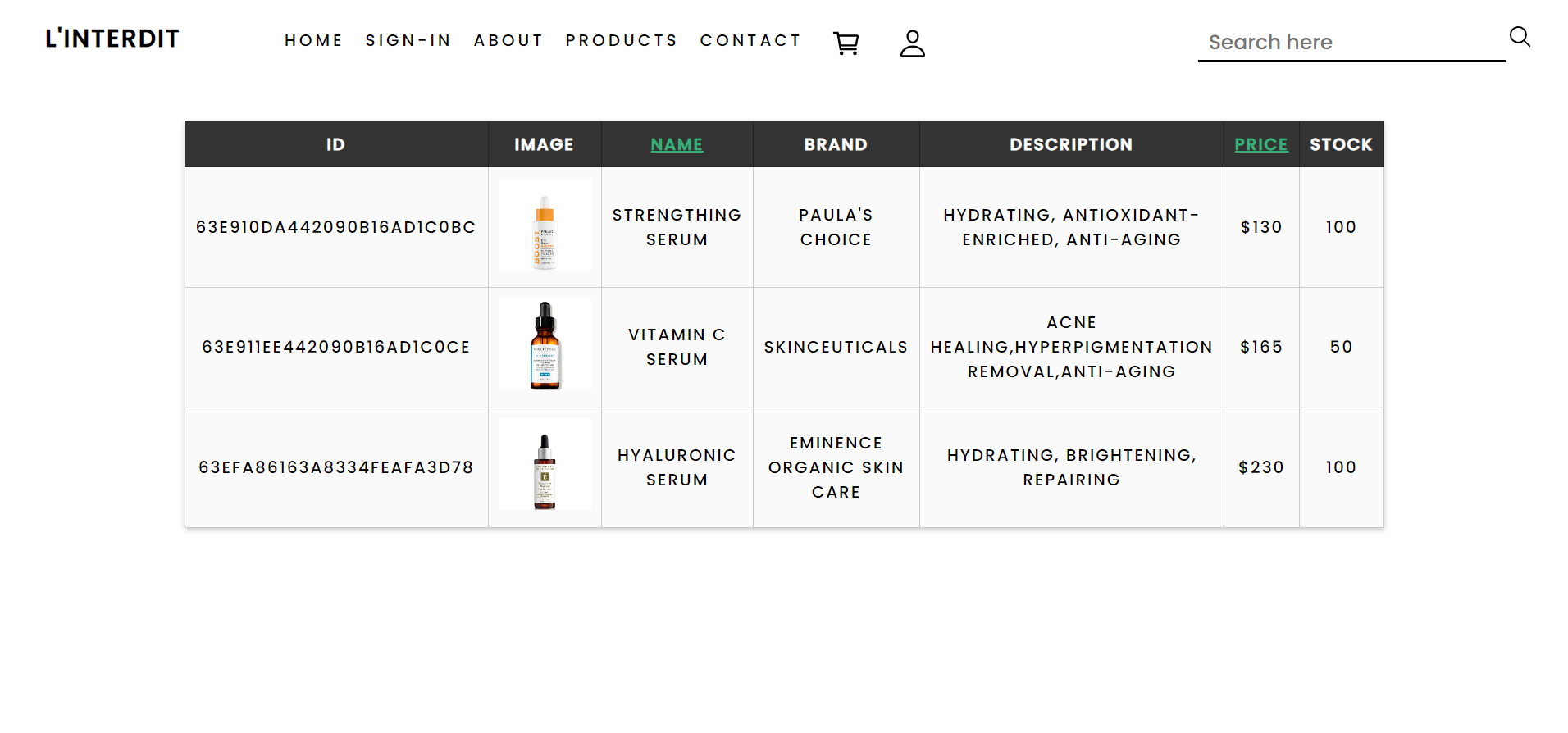


Figure 10: E-commerce searched results

Customers can search for products using keywords or phrases that describe the product through the search bar found at the top of the website. Once the customer has entered the search query, they can click the “search” icon or press “enter” key on their keyboard to display the results in a tabular format.

The customer also has the option to filter their search results either by ascending or descending order of price or by alphabetical order of name. This is made possible by clicking on the headers coloured green on the table.

### Login page

Graphical user interface, text, application

Description automatically generated

Figure 11:E-commerce Login page

A picture containing text

Description automatically generated

A picture containing logo

Description automatically generated

Figure 12: Login error messages

A picture containing graphical user interface

Description automatically generated

Figure 13:Login successful login message

To access the customer dashboard and purchase products, the customer needs to log in. If the user doesn’t have an account, he can click on the “sign up” link to create one.

The customer is prompted to enter his email and password. If the latter is incorrect or the fields are empty, an error message is displayed at the top of the form to indicate so. Once the correct login information is entered, a message is displayed to inform the user.

### Signup page

Graphical user interface, text, application

Description automatically generated

Figure 14: E-commerce Signup page

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

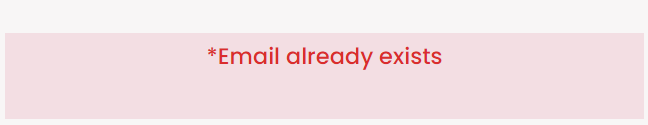
Figure 15: Sign up input validations

A picture containing graphical user interface

Description automatically generated

Graphical user interface, text

Description automatically generated with medium confidence



A picture containing text

Description automatically generated

Figure 16:Sign up error messages

A picture containing graphical user interface

Description automatically generated

Figure 17:Sign up successful registration message

Customers are required to provide their name, email address, password, phone number, and address in order to register.

Error messages will appear at the top of the form or beneath the input fields(for password and phone number) if the customer submits an empty form or if the customer's phone number, email address, or password do not match the allowed format.

Also, if the customer enters an email address that has already been used , an error message will let them know.

An error message will appear if the password and confirmation password entered do not match.

After completing the sign-up process, a message is displayed to indicate so. The customer then needs to log in to browse the website and make purchases, as well as view their profile details and order history.

## CMS (Customer Management System)

The Customer Management System (CMS) is an integral part of our ecommerce store as it allows for the efficient management and maintenance of the store's content. With the CMS website, the staff gain access to a range of functionalities that enable them to effectively view and manage all the orders made by customers.

### Login page

The admin CMS login page allows authorized staff to access and manage the backend of the ecommerce website. It achieves this by comparing the user inputs to the staff accounts stored in the database, and once found, a successful message is displayed, the username is stored as currently logged in staff and access is granted. Without logging in, the staff would not be able to proceed with any action on the CMS page.

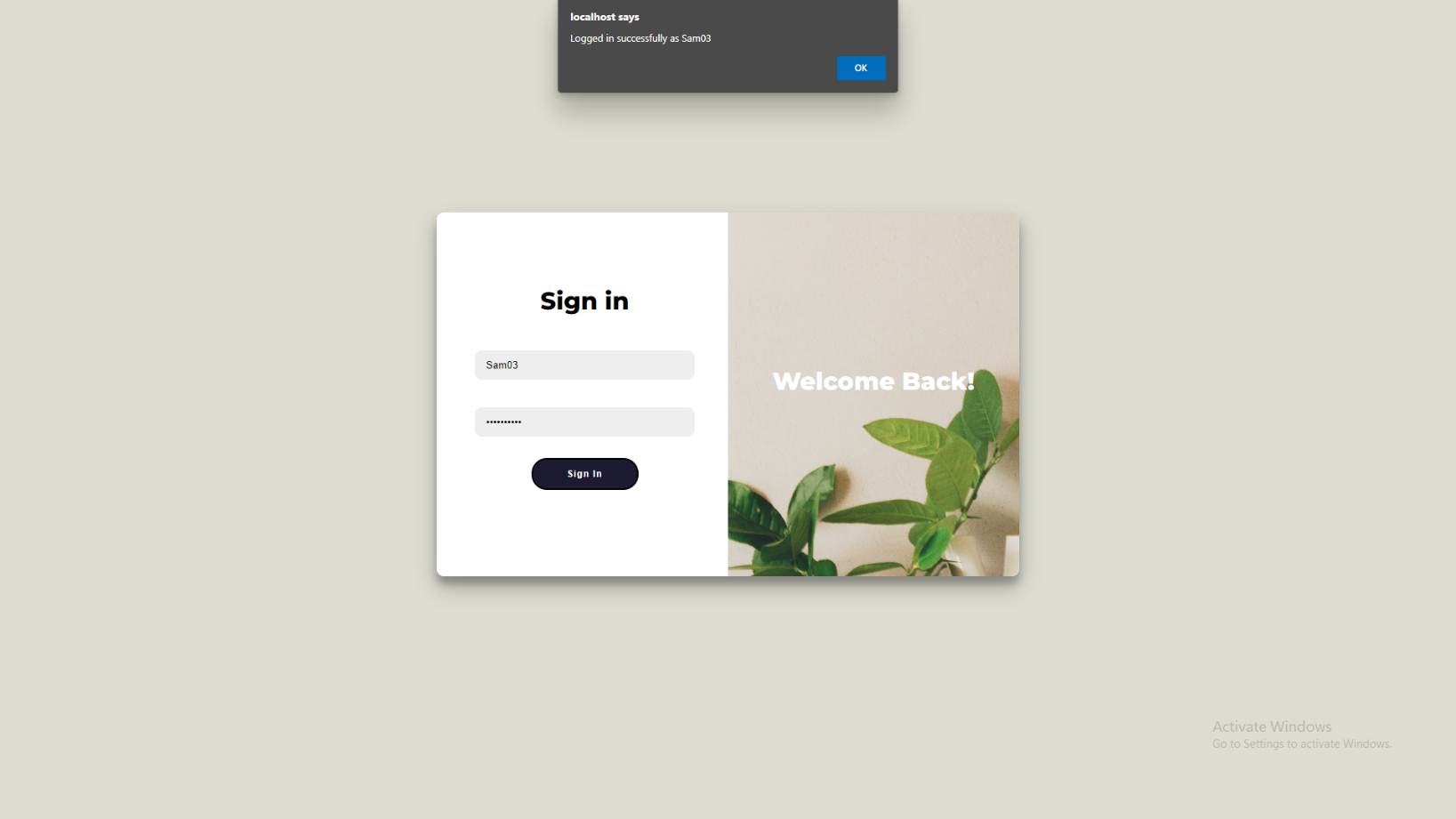
The login page features a simple yet effective design, with a single input field for the user ID and a single input field for the password. This design ensures that logging in is easy and straightforward. It only features a sign in page and no create account page as Admin accounts are pre-set and cannot be created.

Figure 18: CMS Login page

### Home page

This page displays several information to the staff. It shows the total orders made by customers, the total number of products left in the database and the total number of staff available. It then displays a table showing all orders by order ID i.e separated by customer.

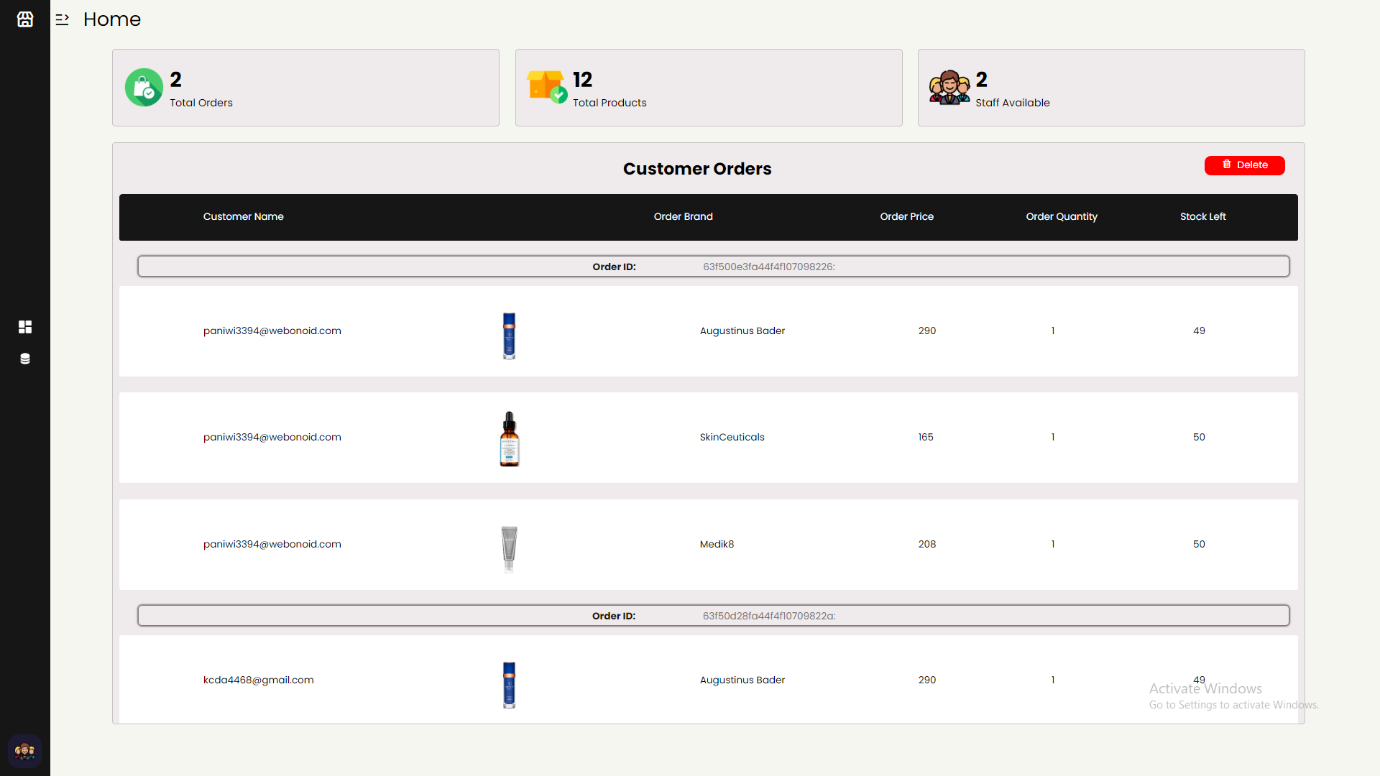


Figure 19: CMS Home page

### Product Page

This page displays all products in the database and allows the user to add all information of a product to the database, edit any data of a product and also delete any product. In order to delete and edit, the ID or the product must be entered.

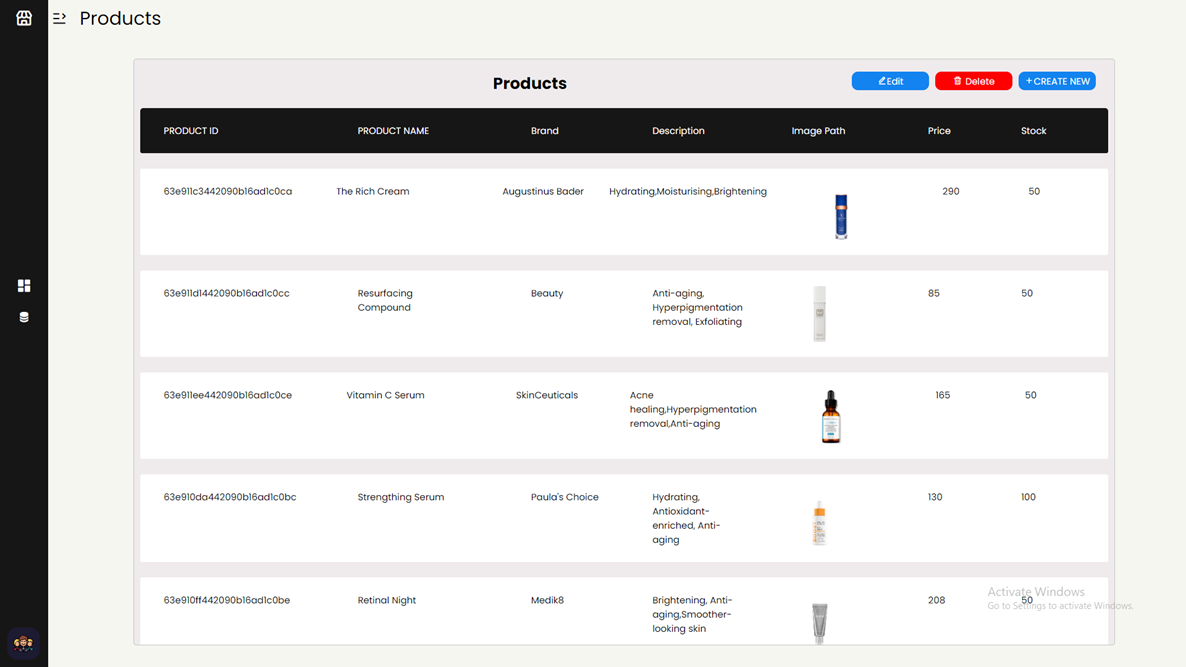


Figure 20:CMS Product page



Figure 21:Add product

A screenshot of a computer

Description automatically generated

Figure 22:Edit product

A screenshot of a computer

Description automatically generated

Figure 23:Delete product

# Security, Privacy and Legal Issues

Implementing security, privacy, and legal features is necessary to safeguard users' sensitive information and adhere to legal requirements as websites have become an integral part of our lives. If not, these could have serious negative impact on website owners and users, such as monetary loss, reputational damage, and legal liabilities. Some of the problems that users could encounter are listed below:

## Security issues

* Insufficient firewalls, a lack of encryption, and poor password restrictions can permit unauthorized access to the website.
* Code injection and cross-site scripting attacks can modify or steal user’s data. By exploiting the login pages and entering PHP scripts or other non-SQL commands in the input boxes to extract all the user's details, the hacker can quickly gain unauthorized access to the database information.
* Hacking, malware, and virus threats can affect user provided sensitive data's availability, confidentiality, and integrity.
* Hackers can obtain private data by creating counterfeit emails or web pages that seem like the real website. These bogus pages might trick users or even website owners into disclosing private information like login information.
* DDoS attacks can be carried out by hackers for a variety of motives, including revenge, extortion, personal, political, or monetary gain. DDoS assaults disrupt web servers by flooding them with excess requests or with packets that aren't properly constructed, rendering websites unreachable.

## Privacy issues

* Collecting, storing (using cookies, local storage, or session storage), and utilizing user’s data without permission.
* Disclosing user information to third parties without the user's permission or in breach of the relevant data protection legislation.
* Failing to give users sufficient control over their personal data, such as the option to delete or update their information.

## Legal issues

* Utilising copyrighted content and photos on the website is illegal and could result in heavy fines.
* Breaking consumer protection rules by using misleading marketing techniques or failing to give customers correct information about products or services
* Contractual violations, such as failing to keep promises given to customers under agreed terms or other agreements.

## How were these issues addressed on the website?

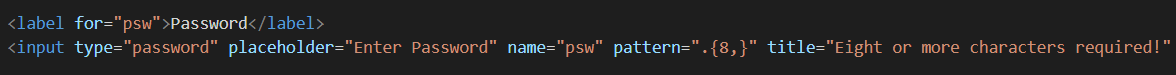
* Passwords must have at least 8 characters, as passwords with more characters have more probable permutations and are therefore more difficult for hackers to decode.

Figure 24:Password validation

* Input validations made sure that the user data was in the right format and was free of malicious code.
* To avoid common web vulnerabilities, secure coding techniques like data sanitization and error handling were utilized. Moreover, PHP and filter input techniques were used to detect malware injection attacks and restrict the storage of unauthorized data.
* To protect against SQL injection attacks, parameterized queries were used.

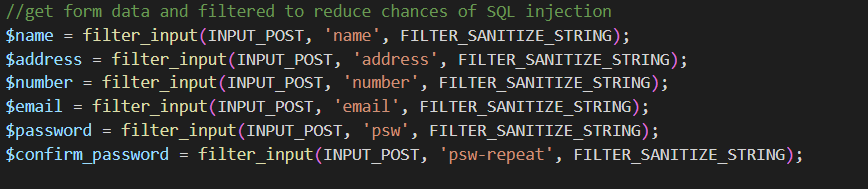


Figure 25; Parameterized query and Data sanitization

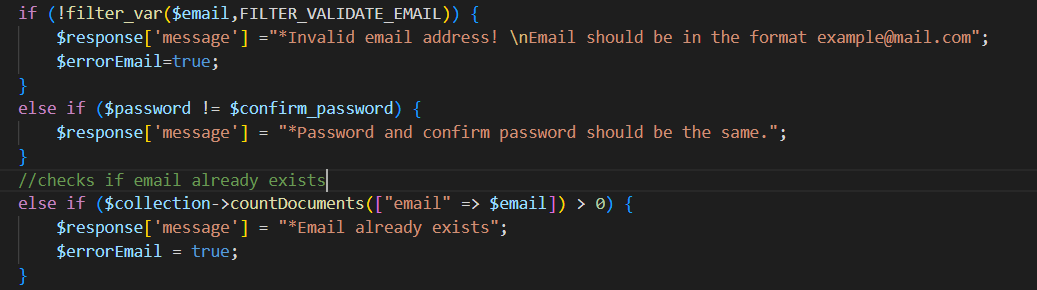


Figure 26: Error handling

* AJAX was used to ensure secure communication between user’s browser and website’s server.

Text

Description automatically generated

Figure 27: AJAX query

* Post method was used instead of GET as POST is a more secure approach since data is not stored in the URL bar.
* PHP session management, which is safe and capable of preventing session hijacking attacks, was chosen over session storage.
* Logging was implemented to track user activity and detect potential security incidents.
* Users with the appropriate permissions can access and change their data.
* Accurate marketing was provided. Customer service is also provided via a "contact us" page.

## How can unresolved issues be addressed in the future?

* The password should be saved in the database in an encrypted or hashed format so that the information is correctly encrypted even if a hacker gains unauthorized access to the database.
* Two-factor authentication and strong passwords can be used to enhance user accounts' security (bcrypt or PBKDF2 can be implemented).
* Rate limiting can be used to avoid brute-force assaults on the login pages and other places where users can enter their information.
* To avoid malicious files from being uploaded to the website, file upload security measures can be put in place. These procedures include limiting file types and sizes and analysing uploaded files for viruses.
* Storing sensitive information, such as credit card numbers, in cookies and local storage needs to be avoided.
* Version control, such as Git, can be used to log changes to website code and easily revert to a previous version if a security issue is identified.
* Regular newsletters can be sent to customers to raise awareness on security issues and remind them to change their passwords.
* Users should be made aware of the information gathered about them, how it is handled, and how it will be used.
* Prior to cookies being kept for tracking and accessing personal information on the website, users should be able to give their consent. A cookie policy should be available.
* The website's database needs to be safe and impenetrable to outsiders. Access to the database should be restricted to authorized individuals only, and it should be encrypted.
* A web application firewall (WAF) can be used to protect against common web attacks such as SQL injection and cross-site scripting.
* If legal permissions have not been obtained, reusing online photos or other materials created by other creators should be avoided.

# References

Mrooms.net. (2023). *Course: 2022-23 CST2120 Web Applications and Databases*. [online] Available at: <https://mdx.mrooms.net/pluginfile.php/3312654/mod_resource/content/3/CSD2550_Lecture27_SecurityPrivacyLegalIssues.pdf> [Accessed 16 Feb. 2023].

Liquid Web. (2021). *Top 15 Most Common Security Issues and How to Fix Them*. [online] Available at: <https://www.liquidweb.com/blog/most-common-web-security-problems/> [Accessed 20 Feb. 2023].

PUREVPN. (2023). *What is internet privacy & why does it matter so much in 2023? - PureVPN Blog*. [online] Available at: <https://www.purevpn.com/blog/what-is-internet-privacy-scty/> [Accessed 20 Feb. 2023].

George van Rooyen (2020). *6 Common Legal Issues Around Website Content*. [online] Pagefreezer.com. Available at: <https://blog.pagefreezer.com/common-legal-issues-web-content> [Accessed 20 Feb. 2023].

‌

‌

‌

‌

‌

‌