

VIETNAM NATIONAL UNIVERSITY, HO CHI MINH CITY
UNIVERSITY OF TECHNOLOGY
FACULTY OF COMPUTER SCIENCE AND ENGINEERING



BÁO CÁO BÀI TẬP LỚN

Lập Trình Web (CO3049)

GVHD: NGUYỄN HỮU HIẾU

SVTH: Bùi Tiến Lộc – 2013678
Phạm Cảnh Hưng – 2010029
Bùi Quang Khải – 2013470

Tp. Hồ Chí Minh, Tháng 4/2023

Mục lục

1	Tổng quát về bài toán	3
1.1	Đặt vấn đề	3
1.2	Mô tả hoạt động của cửa hàng	3
1.2.1	Ban điều hành	3
1.2.2	Bộ phận bán hàng	3
1.2.3	Bộ phận quản trị	4
1.3	Yêu cầu của hệ thống bán hàng qua mạng	4
1.3.1	Nhu cầu người sử dụng	4
1.3.2	Nhu cầu người quản trị	4
2	Cơ Sở Lý Thuyết	4
2.1	Thư viện & Công nghệ sử dụng	4
2.1.1	Công nghệ Web HTML5 + CSS3	4
2.1.2	Công nghệ Web PHP + MySQL	7
2.1.3	Bootstrap	9
2.2	Các lỗ hổng bảo mật trong ứng dụng Web	10
2.2.1	Lỗ hổng Injection (Lỗi chèn mã độc)	10
2.2.2	Broken Authentication	10
2.2.3	Lỗ hổng XSS (Cross Site Scripting)	11
2.2.4	Insecure Direct Object References	11
2.2.5	Security Misconfiguration	11
2.2.6	Sensitive data exposure (Rò rỉ dữ liệu nhạy cảm)	12
2.2.7	Missing function level access control (lỗi phân quyền)	12
2.2.8	Cross Site Request Forgery (CSRF)	12
2.2.9	Using component with known vulnerabilities	13
2.2.10	Unvalidated redirects and forwards	13
2.3	SEO đối với Website	13
3	Thiết Kế cơ sở dữ liệu	15
3.1	Mô hình thực thể liên kết	15
3.2	Quản trị viên (admin)	15
3.3	Bài viết	16
3.4	Thương hiệu	16
3.5	Giỏ hàng	17
3.6	Danh mục	17
3.7	Khách hàng	18
3.8	Chi tiết giỏ hàng	18
3.9	Chi tiết đơn hàng	19
3.10	Đơn hàng	19
3.11	Sản phẩm	20
3.12	Slider	20
3.13	Bình luận	21
3.14	Thông tin cửa hàng	21
4	Hiện Thực	21
5	Kết luận, hướng dẫn sử dụng và cài đặt	21
5.1	Kết luận	21
5.1.1	Những công việc đã làm được	21
5.1.2	Hạn chế	22
5.1.3	Kết luận	22
5.2	Hướng dẫn sử dụng và cài đặt	22
5.2.1	Hướng dẫn sử dụng	22
5.2.1.a	Vào trang web	22



5.2.1.b	Tìm kiếm sản phẩm	22
5.2.1.c	Đặt hàng	23
5.2.1.d	Các chức năng của quản trị viên	25
5.2.2	Hướng dẫn cài đặt	26
Tài liệu tham khảo		29

1 Tổng quát về bài toán

1.1 Đặt vấn đề

Ngày nay, công nghệ thông tin đã có những bước phát triển mạnh mẽ theo cả chiều rộng và sâu. Máy tính điện tử không còn là một thứ phương tiện quý hiếm mà đang ngày càng trở thành một công cụ làm việc và giải trí thông dụng của con người, không chỉ ở nơi làm việc mà còn ngay cả trong gia đình. Đặc biệt là công nghệ thông tin được áp dụng trên mọi lĩnh vực kinh tế, chính trị, xã hội Ứng dụng công nghệ thông tin và tin học hóa được xem là một trong yếu tố mang tính quyết định trong hoạt động của quốc gia, tổ chức và trong cả các cửa hàng. Nó đóng vai trò hết sức quan trọng và có thể tạo nên bước đột phá mạnh mẽ.

Mạng INTERNET là một trong những sản phẩm có giá trị hết sức lớn lao và ngày càng trở nên một công cụ không thể thiếu, là nền tảng để truyền tải, trao đổi thông tin trên toàn cầu. Bằng INTERNET, chúng ta đã thực hiện được những công việc với tốc độ nhanh hơn, chi phí thấp hơn nhiều so với cách thức truyền thống. Chính điều này, đã thúc đẩy sự khai sinh và phát triển của thương mại điện tử trên khắp thế giới, làm biến đổi đáng kể bộ mặt văn hóa, nâng cao đời sống con người. Trong hoạt động sản xuất, kinh doanh, thương mại điện tử đã khẳng định được xúc tiến và thúc đẩy sự phát triển của doanh nghiệp. Đối với một cửa hàng, việc quảng bá và giới thiệu sản phẩm đến khách hàng đáp ứng nhu cầu mua sắm ngày càng cao của khách hàng sẽ là cần thiết. Vì vậy, nhóm chúng em đã thực hiện đề tài “**Xây dựng Website bán quần áo**”. Cửa hàng có thể đưa các sản phẩm lên Website của mình và quản lý Website đó, khách hàng có thể đặt mua, mua hàng của cửa hàng mà không cần đến cửa hàng, cửa hàng sẽ gửi sản phẩm đến tận tay khách hàng. Website là nơi cửa hàng quảng bá tốt nhất tất cả các sản phẩm mình bán ra.

Mục tiêu xây dựng trang web này nhằm giúp cho khách hàng có thể mua hàng trực tiếp từ xa thông qua mạng internet. Khách hàng ở nhà hay tại cửa hàng vẫn có thể dễ dàng tham khảo thông tin sản phẩm mình tìm, so sánh giá cả các mặt hàng và lựa chọn cho mình loại sản phẩm phù hợp nhu cầu của mình, giúp công việc mua sắm một cách nhanh chóng, tiện lợi, tiết kiệm thời gian, đáp ứng được nhu cầu thực tế. Hệ thống tìm kiếm dễ dàng, giao diện thân thiện. Chỉ cần đăng nhập vào hệ thống với tài khoản đã có hay chỉ cần vài thao tác đăng kí đơn giản là khách hàng có thể tự do chọn mua và tạo đơn đặt hàng tại hệ thống.

1.2 Mô tả hoạt động của cửa hàng

1.2.1 Bàn điều hành

- Quản lý và phân phối hoạt động của cửa hàng.
- Quyết định giá chính thức cho từng mặt hàng.

1.2.2 Bộ phận bán hàng

- Bán hàng qua mạng là một hình thức mới mà người mua hàng phải tự thao tác thông qua từng bước để có thể mua được hàng.
- Các sản phẩm được sắp xếp, phân chia theo nhiều chủng loại hàng hóa và có nhiều mặt hàng khác nhau để giúp cho người dùng dễ sử dụng, giúp cho người quản trị dễ thay thế, thêm bớt sản phẩm của mình. Trong cách này, người dùng chỉ cần chọn một sản phẩm nào từ trong danh sách của từng loại sản phẩm thì những thông tin về loại sản phẩm đó sẽ hiện lên theo tên hàng hóa, hình ảnh, giá bán và nhưng mô tả ngắn về loại thiết bị đó, bên cạnh là trang liên kết để thêm sản phẩm vào trong giỏ mua hàng.
- Giỏ hàng chứa các thông tin lần số lượng hàng hóa người dùng mua và có thể được cập nhật vào trong giỏ.
- Khi khách hàng muốn đặt hàng thì hệ thống hiển thị trang xác lập đơn đặt hàng cùng với thông tin về khách hàng và hàng hóa.

1.2.3 Bộ phận quản trị

Công việc của bộ phận này là thực hiện các nhiệm vụ quản trị mạng, quản lý thông tin của khách hàng, cập nhật thông tin của sản phẩm,... đảm bảo cơ sở dữ liệu luôn được cập nhật nhanh chóng.

1.3 Yêu cầu của hệ thống bán hàng qua mạng

1.3.1 Nhu cầu người sử dụng

- Nhu cầu của khách hàng khi truy cập vào trang web là tìm kiếm các sản phẩm. Do đó yêu cầu của chương trình là phải đáp ứng được những nhu cầu đó, sao cho khách hàng có thể tìm kiếm nhanh chóng và hiệu quả các loại sản phẩm mà họ muốn và cần mua.
- Chương trình phải có tính đa dạng và hấp dẫn nhằm thu hút sự quan tâm của nhiều người về công ty mình.
- Trang web phải dễ hiểu, giao diện phải dễ dùng, hấp dẫn và quan trọng là làm sao cho khách thấy những thông tin cần tìm cũng như thông tin liên quan.
- Điều quan trọng trong mua bán qua mạng là phải đảm bảo an toàn tuyệt đối những thông tin liên quan đến người dùng trong quá trình đặt mua hay thanh toán cũng được đảm bảo hàng được chuyển giao đúng nơi, đúng lúc.

1.3.2 Nhu cầu người quản trị

Trang web đòi hỏi người quản trị phải thường xuyên theo dõi các thông tin về hàng hóa, xử lý đúng yêu cầu, đúng chức năng do mình nhập vào và thao tác dễ dàng với công việc quản lý dữ liệu:

- Được phép chỉnh sửa, xóa những thông tin sai, không phù hợp.
- Theo dõi quá trình mua bán.
- Theo dõi thông tin khách hàng nhập vào khi mua hàng, phải đảm bảo tính an toàn, bảo mật, chính xác.
- Theo dõi, xử lý các đơn đặt hàng và cập nhật các thông tin liên quan đến đơn đặt hàng của khách.
- Có thể xóa tất cả các cơ sở dữ liệu sau một thời gian xác định.

2 Cơ Sở Lý Thuyết

2.1 Thư viện & Công nghệ sử dụng

2.1.1 Công nghệ Web HTML5 + CSS3

HTML hay HyperText Markup Language, là thành phần quan trọng nhất của World Wide Web. Nó là ngôn ngữ dùng để mô tả những gì một trang web hiển thị. Tuy nhiên, nếu chỉ riêng HTML thôi thì khá nhàm chán bởi vì nó chỉ có thể cung cấp các trang web tĩnh; nhằm đáp ứng nhu cầu ngày càng tăng về các tính năng web ấn tượng hơn, HTML đã được kết hợp với các plugin như CSS, Flash, Java, Silverlight, v.v...

Nó đã trở thành một cái gì đó khá công kênh và các trình duyệt khác nhau thực hiện những tính năng theo cách riêng của chúng. HTML5 sinh ra để giải quyết những vấn đề lớn của HTML, giúp cho trang web trở nên rõ ràng và hiệu quả hơn.

Ưu điểm vượt trội của HTML5 so với các phiên bản trước:

- HTML5 hỗ trợ cho nhiều ứng dụng hơn: Một số ứng dụng như SVG, canvas... được HTML5 hỗ trợ, nhưng dùng trong HTML thì phải sử dụng thêm các phương tiện bổ trợ.



Hình 1: Biểu tượng của HTML5

- Lưu dữ liệu tạm: HTML5 sử dụng web SQL databases, application cache còn HTML chỉ dùng cache của trình duyệt.
- JavaScript chạy trong web browser: HTML5 hỗ trợ hoàn toàn cho JavaScript chạy trên web browser, còn HTML ở các phiên bản cũ hơn thì không thể thực hiện được.
- HTML5 không dựa trên SGML, nhờ vậy, sản phẩm lập trình có độ tương thích cao hơn.
- HTML5 cho phép sử dụng MathML và SVG cho văn bản, nhưng trong HTML thì không được hỗ trợ.
- HTML5 tích hợp các element mới mẻ và quan trọng như summary, time, aside, audio, command, data, datalist, details, embed, wbr, figcaption, figure, footer, header, article, hgroup, bdi, canvas, keygen, mark, meter, nav, output, progress, rp, rt, ruby, section, source, track, video... Bên cạnh đó, nó cũng được loại bỏ các elements lỗi thời trong HTML như isindex, noframes, acronym, applet, basefont, dir, font, frame, frameset, big, center, strike...
- HTML5 còn giúp người dùng cuối cảm thấy thoải mái, dễ dàng hơn trong quá trình truy cập website trên cả PC và mobile. Người dùng không cần tải ứng dụng vẫn có thể dễ dàng truy cập được website. Và tìm hiểu tất cả thông tin. Người dùng cuối không cần tải plugin đi kèm vẫn có thể xem được các thông tin đa phương tiện (multimedia) trên website.

Tuy nhiên vì là công nghệ mới nên HTML5 vẫn còn một số hạn chế như:

- Nhiều trình duyệt vẫn còn chậm trong việc hỗ trợ các tính năng mới của HTML5.
- Một số trình duyệt cũ vẫn không thể render được những tag mới có bên trong HTML5.

CSS là từ viết tắt của cụm từ Cascading Style Sheets, ngôn ngữ được sử dụng để tạo nên phong cách cho website.

Có thể hiểu CSS đóng vai trò như một công cụ giúp chúng ta thêm vào những thay đổi về mặt hình thức như đối bố cục, màu sắc, font chữ,... CSS hoạt động bằng cách khoanh vùng chọn dựa vào tên một thẻ HTML, ID hay Class. Từ đó, áp dụng những thuộc tính cần thay đổi lên vùng được chọn. Nếu một website không có CSS thì đó sẽ chỉ đơn thuần là một trang chứa văn bản với 2 màu chủ đạo là trắng và đen.

CSS3 là phiên bản thứ 3 và cũng là mới nhất của CSS, CSS3 được bổ sung thêm nhiều tính năng mới tiện lợi hơn CSS cho người dùng. Được thừa hưởng tất cả những gì có trong phiên bản trước và bổ



Hình 2: Biểu tượng của CSS3

sung các tính năng mới, CSS3 hiện rất được ưa chuộng trong thiết kế website.

Ưu điểm có thể kể đến của CSS3 như:

- Tương thích với HTML5: Khi mà HTML5 đang dần thay thế Flash, thì CSS3 chính là sự hỗ trợ cần thiết để có một giao diện website hoàn hảo.
- Hiển thị cho các thiết bị có kích thước khác nhau: Media Queries mới ra mắt trong CSS3 là bước ngoặt lớn cho các website. Hỗ trợ tương thích với các kích thước màn hình mà không cần chỉnh sửa nội dung hiển thị.
- Tối ưu hóa công cụ tìm kiếm SEO: Một điểm mạnh nữa của CSS3 được rất nhiều lập trình viên ưa chuộng là khả năng loại bỏ những đoạn code HTML bị thừa. Giúp các công cụ tìm kiếm có thể hoạt động tốt hơn.
- Tương thích với trình duyệt: CSS3 cũng được đánh giá rất cao về khả năng tương thích khi có thể hoạt động tốt trên hầu hết các trình duyệt phổ biến. Dù hiển thị trên nhiều trình duyệt khác nhau nhưng website vẫn khá nhất quán.
- Ngoài ra, CSS3 còn hỗ trợ nhiều tính năng mới như: Bộ chọn, CSS3 Pseudo-Classes, Màu trong CSS3, CSS3 RGBA, CSS3 HSL và HSLA, CSS3 Opacity,...



Hình 3: HTML5 kết hợp CSS3

HTML5 kết hợp CSS3 đã trở thành một tiêu chuẩn của thiết kế web, giúp lập trình viên dễ dàng hơn trong việc thiết kế cũng như cải thiện trang web của mình. Ngoài ra, trải nghiệm người dùng ngày càng được nâng cao khi không cần phải luôn để ý đến các bản cập nhật của các plugin như Flash và Java...

2.1.2 Công nghệ Web PHP + MySQL



Hình 4: Ngôn ngữ PHP

PHP là một từ viết tắt của cụm từ Hypertext Pre Processor. Là một ngôn ngữ lập trình thường được sử dụng để phát triển ứng dụng. Những thứ có liên quan đến viết máy chủ, mã nguồn mở hay mục đích tổng quát. Ngoài ra, nó còn rất thích hợp để lập trình web và có thể dễ dàng nhúng vào trang HTML. Ngày nay, PHP đã chiếm tới hơn 70% web hiện nay, trang web giới thiệu của các công ty như influxwebtechnologies, Monamedia đều được xây dựng bằng WordPress – một mã nguồn được viết bởi ngôn ngữ PHP. Bởi những tính năng như tối ưu hóa cho các ứng dụng web. Tốc độ load web nhanh, nhỏ gọn, cú pháp giống C và JAVA. Rất dễ học và thời gian xây dựng sản phẩm tương đối ngắn hơn so với các ngôn ngữ khác hiện nay.

PHP có những ưu điểm chính có thể kể đến như:

- PHP là ngôn ngữ mã nguồn mở được sử dụng miễn phí với kho tài liệu khổng lồ cũng như cộng đồng lớn.
- Cú pháp và cấu trúc của PHP tương đối dễ dàng.
- Có thể lồng ghép mã HTML vào trong.

Tuy nhiên, do là một ngôn ngữ lâu đời nên PHP có một số hạn chế như:

- PHP có hạn chế về cấu trúc ngữ pháp, bởi nó không được thiết kế gọn gàng và đẹp mắt như những loại ngôn ngữ khác
- PHP chỉ có thể hoạt động và sử dụng cho các ứng dụng trên web. Đó chính là hạn chế cần khắc phục nếu muốn cạnh tranh và phát triển rộng rãi hơn nữa so với các ngôn ngữ lập trình khác.
- Server bằng PHP thường chậm và khả năng chịu tải không cao.

MySQL là một hệ thống quản trị cơ sở dữ liệu mã nguồn mở (Relational Database Management System – được gọi tắt là RDBMS). Hệ thống hoạt động theo mô hình client – server, dựa trên ngôn ngữ truy vấn có cấu trúc (SQL) và được phát triển, phân phối, hỗ trợ bởi Tập đoàn Oracle.

MySQL được ưa chuộng trong quá trình xây dựng và phát triển các ứng dụng. Hệ thống quản trị cơ sở dữ liệu này được đánh giá có tốc độ cao, ổn định, dễ dùng và có khả năng thay đổi mô hình sử dụng



Hình 5: Cơ sở dữ liệu MySQL

phù hợp với điều kiện công việc.

MySQL hiện đang hoạt động trên nhiều hệ điều hành Linux, Unix, Windows, ..., cung cấp một hệ thống lớn các hàm tiện ích mạnh mẽ. Nó thích hợp với các ứng dụng có truy cập cơ sở dữ liệu trên internet nhờ tốc độ cao và tính bảo mật tốt. Người dùng có thể tải miễn phí MySQL từ trang chủ với nhiều phiên bản cho các hệ điều hành khác nhau.

MySQL sở hữu nhiều ưu điểm riêng giúp người dùng nhiều công việc như:

- Miễn phí: MySQL được phát hành theo giấy phép nguồn mở. Bởi vậy, ta không phải trả tiền để sử dụng nó.
- Dễ sử dụng: Nó hoạt động trên nhiều hệ điều hành với nhiều ngôn ngữ bao gồm Java, C, C++, PHP, ... Bởi vậy, nó cung cấp một hệ thống các hàm tiện ích mạnh mẽ và tiện lợi.
- Tốc độ nhanh chóng: MySQL là hệ cơ sở dữ liệu dễ dùng, có tốc độ nhanh và hoạt động ổn định ngay cả với các tập dữ liệu lớn.
- Hỗ trợ cơ sở dữ liệu lớn: MySQL có thể hỗ trợ cơ sở dữ liệu lên tới 50 triệu hoặc nhiều hơn trong một bảng. Giới hạn kích thước tệp mặc định cho 1 bảng là 4GB nhưng có thể tăng hạn mức nếu hệ điều hành có xử lý được. Giới hạn lý thuyết có thể lên tới 8 triệu TB.
- Chương trình mạnh mẽ: MySQL là một chương trình mạnh mẽ theo đúng nghĩa. Nó có thể xử lý một tập hợp lớn các chức năng của các gói cơ sở dữ liệu mạnh mẽ và đắt tiền nhất.
- Tính bảo mật cao: MySQL sở hữu nhiều tính năng bảo mật cấp cao. Bởi vậy, nó cực kỳ thích hợp cho các ứng dụng có truy cập cơ sở dữ liệu trên internet.
- Đa tính năng: MySQL hỗ trợ nhiều chức năng SQL được mong chờ từ một hệ quản trị CSDL quan hệ cả trực tiếp và gián tiếp.
- Khả năng tùy biến cao: Giấy phép GPL mã nguồn mở cho phép các lập trình viên sửa đổi phần mềm MySQL sao cho phù hợp với môi trường sử dụng của riêng họ.

Ngoài những ưu điểm vượt trội, MySQL cũng vướng phải một số hạn chế nhất định như:

- Độ tin cậy chưa cao: Do các chức năng cụ thể được xử lý với MySQL (giao dịch, kiểm toán, tài liệu tham khảo, ...) khiến cho nó kém tin cậy hơn so với một số hệ quản trị CSDL khác.
- Giới hạn: MySQL sẽ không làm tất cả và nó sẽ đi kèm một số hạn chế nhất định về chức năng mà một ứng dụng có thể cần đến.

- Hạn chế truy xuất khi dung lượng lớn: Nếu bản ghi lớn dần lên thì việc truy xuất dữ liệu sẽ khó khăn hơn. Khi đó, ta phải áp dụng nhiều biện pháp nhằm tăng tốc độ truy xuất dữ liệu (ví dụ như: chia tải database ra nhiều server, tạo cache MySQL,...).

2.1.3 Bootstrap

Bootstrap là gì?

Bootstrap là 1 framework HTML, CSS, và JavaScript cho phép người dùng dễ dàng thiết kế website theo 1 chuẩn nhất định, tạo các website thân thiện với các thiết bị cầm tay như mobile, ipad, tablet,...

Tại sao nên sử dụng Bootstrap?

Bootstrap là một trong những framework được sử dụng nhiều nhất trên thế giới để xây dựng nên một website. Bootstrap đã xây dựng nên 1 chuẩn riêng và rất được người dùng ưa chuộng. Chính vì thế, chúng ta hay nghe tới một cụm từ rất thông dụng "Thiết kế theo chuẩn Bootstrap".



Lợi ích khi sử dụng Bootstrap

- Rất dễ để sử dụng: Nó đơn giản vì nó được base trên HTML, CSS và Javascript chỉ cần có kiến thức cơ bản về 3 cái đó là có thể sử dụng bootstrap tốt.
- Responsive: Bootstrap xây dựng sẵn responsive css trên các thiết bị Iphones, tablets, và desktops. Tính năng này khiến cho người dùng tiết kiệm được rất nhiều thời gian trong việc tạo ra một website thân thiện với các thiết bị điện tử, thiết bị cầm tay.
- Tương thích với trình duyệt: Nó tương thích với tất cả các trình duyệt (Chrome, Firefox, Internet Explorer, Safari, and Opera). Tuy nhiên, với IE browser, Bootstrap chỉ hỗ trợ từ IE9 trở lên. Điều này vô cùng dễ hiểu vì IE8 không support HTML5 và CSS3.

Nhược điểm

- Nặng, tốc độ tối ưu chưa cao: Đây là một điểm trừ khá lớn cho Bootstrap, bởi framework của nó ôm quá nhiều chức năng tổng dung lượng lên tới gần 7MB.

- Chưa hoàn thiện: Hiện nay, Bootstrap vẫn đang tiếp tục phát triển chưa có đầy đủ các thư viện cần thiết để tạo ra một framework hoàn hảo.
- Nhiều code thừa: Bootstrap cung cấp gần như đầy đủ những tính năng cơ bản của một trang web responsive hiện đại. Tuy nhiên, mặt trái của việc này là website của bạn sẽ phải tải thêm rất nhiều dòng code không cần thiết khi mà bạn chỉ cần chưa đến 10% những gì Bootstrap cung cấp.
- Hạn chế sáng tạo: Bootstrap không khuyến khích sáng tạo: Chỉ cần nhét Bootstrap vào themes sẵn có, gọi ra cái .class từ stylesheet và thế là bạn đã có một trang web responsive. Tuy vậy các theme này sẽ khiến bạn gò bó và khó sáng tạo hơn.

2.2 Các lỗ hổng bảo mật trong ứng dụng Web

2.2.1 Lỗ hổng Injection (Lỗi chèn mã độc)

Injection là lỗ hổng xảy ra do sự thiếu sót trong việc lọc các dữ liệu đầu vào không đáng tin cậy. Khi bạn truyền các dữ liệu chưa được lọc tới Database (Ví dụ như lỗ hổng SQL injection), tới trình duyệt (lỗ hổng XSS), tới máy chủ LDAP (lỗ hổng LDAP Injection) hoặc tới bất cứ vị trí nào khác. Vấn đề là kẻ tấn công có thể chèn các đoạn mã độc để gây ra lộ lọt dữ liệu và chiếm quyền kiểm soát trình duyệt của khách hàng.

Mọi thông tin mà ứng dụng của bạn nhận được đều phải được lọc theo Whitelist. Bởi nếu bạn sử dụng Blacklist việc lọc thông tin sẽ rất dễ bị vượt qua (Bypass). Tính năng Pattern matching sẽ không hoạt động nếu thiết lập Blacklist.

Cách ngăn chặn lỗ hổng:

Để chống lại lỗ hổng này chỉ “đơn giản” là vấn đề bạn đã lọc đầu vào đúng cách chưa hay việc bạn cân nhắc liệu một đầu vào có thể được tin cậy hay không. Về căn bản, tất cả các đầu vào đều phải được lọc và kiểm tra trừ trường hợp đầu vào đó chắc chắn đáng tin cậy. (Tuy nhiên việc cẩn thận kiểm tra tất cả các đầu vào là luôn luôn cần thiết).

Ví dụ, trong một hệ thống với 1000 đầu vào, lọc thành công 999 đầu vào là không đủ vì điều này vẫn để lại một phần giống như “gót chân Asin”, có thể phá hoại hệ thống của bạn bất cứ lúc nào. Bạn có thể cho rằng đưa kết quả truy vấn SQL vào truy vấn khác là một ý tưởng hay vì cơ sở dữ liệu là đáng tin cậy. Nhưng thật không may vì đầu vào có thể gián tiếp đến từ những kẻ có ý đồ xấu. Đây được gọi là lỗi Second Order SQL Injection.

Việc lọc dữ liệu khá khó vì thế các bạn nên sử dụng các chức năng lọc có sẵn trong framework của mình. Các tính năng này đã được chứng minh sẽ thực hiện việc kiểm tra một cách kỹ lưỡng. Bạn nên cân nhắc sử dụng các framework vì đây là một trong các cách hiệu quả để bảo vệ máy chủ của bạn.

2.2.2 Broken Authentication

Đây là nhóm các vấn đề có thể xảy ra trong quá trình xác thực. Có một lời khuyên là không nên tự phát triển các giải pháp mã hóa vì rất khó có thể làm được chính xác.

Có rất nhiều rủi ro có thể gặp phải trong quá trình xác thực:

- URL có thể chứa Session ID và rò rỉ nó trong Referer Header của người dùng khác.
- Mật khẩu không được mã hóa hoặc dễ giải mã trong khi lưu trữ.
- Lỗ hổng Session Fixation.
- Tấn công Session Hijacking có thể xảy ra khi thời gian hết hạn của session không được triển khai đúng hoặc sử dụng HTTP (không bảo mật SSL)...

Cách ngăn chặn lỗ hổng:

Cách đơn giản nhất để tránh lỗ hổng bảo mật web này là sử dụng một framework. Trong trường hợp bạn muốn tự tạo ra bộ xác thực hoặc mã hóa cho riêng mình, hãy nghĩ đến những rủi ro mà bạn sẽ gặp phải và tự cân nhắc kỹ trước khi thực hiện.

2.2.3 Lỗ hổng XSS (Cross Site Scripting)

Lỗ hổng XSS (Cross-site Scripting) là một lỗ hổng rất phổ biến. Kẻ tấn công chèn các đoạn mã JavaScript vào ứng dụng web. Khi đầu vào này không được lọc, chúng sẽ được thực thi mã độc trên trình duyệt của người dùng. Kẻ tấn công có thể lấy được cookie của người dùng trên hệ thống hoặc lừa người dùng đến các trang web độc hại.

Cách ngăn chặn lỗ hổng:

Có một cách bảo mật web đơn giản đó là không trả lại thẻ HTML cho người dùng. Điều này còn giúp chống lại HTML Injection – Một cuộc tấn công tương tự mà hacker tấn công vào nội dung HTML – không gây ảnh hưởng nghiêm trọng nhưng khá rắc rối cho người dùng. Thông thường cách giải quyết đơn giản chỉ là Encode (chuyển đổi về dạng dữ liệu khác) tất cả các thẻ HTML. Ví dụ thẻ `<script>` được trả về dưới dạng `<script>`.

2.2.4 Insecure Direct Object References

Đây là trường hợp điển hình của việc cho rằng đầu vào của người dùng là tin cậy từ đó dẫn đến lỗ hổng bảo mật. Lỗ hổng này xảy ra khi chương trình cho phép người dùng truy cập các tài nguyên (dữ liệu, file, database). Nếu không thực hiện quá trình kiểm soát quyền hạn (hoặc quá trình này không hoàn chỉnh) kẻ tấn công có thể truy cập một cách bất hợp pháp vào các dữ liệu nhạy cảm, quan trọng trên máy chủ.

Chúng ta có thể xem xét ví dụ sau:

Một đoạn mã có module `download.php` và cho phép người dùng tải tệp xuống sử dụng tham số CGI. Ví dụ `download.php?file=something.txt`. Do sai sót của nhà phát triển, việc kiểm tra quyền hạn đã bị bỏ qua. Kẻ tấn công có thể sử dụng lỗ hổng này để tải về bất kì tệp nào trên hệ thống mà ứng dụng có quyền truy cập. Chẳng hạn như code ứng dụng, hoặc các dữ liệu khác trên máy chủ.

Một ví dụ phổ biến khác là chức năng đặt lại mật khẩu dựa vào đầu vào của người dùng để xác định mật khẩu đặt lại. Sau khi nhập vào URL hợp lệ, kẻ tấn công có thể sửa đổi trường tên người dùng trong URL để “đóng giả” admin.

Cách ngăn chặn lỗ hổng:

Thực hiện phân quyền người dùng đúng cách và nhất quán với sự áp dụng triệt để các Whitelist.

2.2.5 Security Misconfiguration

Trong thực tế, máy chủ website và các ứng dụng đa số bị cấu hình sai. Có lẽ do một vài sai sót như:

- Chạy ứng dụng khi chế độ debug được bật.
- Directory listing
- Sử dụng phần mềm lỗi thời (WordPress plugin, PhpMyAdmin cũ)
- Cài đặt các dịch vụ không cần thiết.
- Không thay đổi default key hoặc mật khẩu
- Trả về lỗi xử lý thông tin cho kẻ tấn công lợi dụng để tấn công, chẳng hạn như stack traces.

Cách ngăn chặn lỗ hổng:

Có một quá trình xây dựng ứng dụng an toàn. Cần một quá trình audit lỗ hổng bảo mật trên máy chủ trước khi triển khai.

2.2.6 Sensitive data exposure (Rò rỉ dữ liệu nhạy cảm)

Lỗ hổng này thuộc về khía cạnh crypto và tài nguyên. Dữ liệu nhạy cảm phải được mã hóa mọi lúc, bao gồm cả khi gửi đi và khi lưu trữ – không được phép có ngoại lệ. Thông tin thẻ tín dụng và mật khẩu người dùng không bao giờ được gửi đi hoặc được lưu trữ không được mã hóa. Rõ ràng thuật toán mã hóa và hashing không phải là một cách bảo mật yếu. Ngoài ra, các tiêu chuẩn an ninh web đề nghị sử dụng AES (256 bit trở lên) và RSA (2048 bit trở lên).

Cần phải nói rằng các Session ID và dữ liệu nhạy cảm không nên được truyền trong các URL và cookie nhạy cảm nên có cờ an toàn.

Cách ngăn chặn lỗ hổng:

- Sử dụng HTTPS có chứng chỉ phù hợp và PFS (Perfect Forward Secrecy). Không nhận bất cứ thông tin gì trên các kết nối không phải là HTTPS. Có cờ an toàn trên cookie.
- Bạn cần hạn chế các dữ liệu nhạy cảm có khả năng bị lộ của mình. Nếu bạn không cần những dữ liệu nhạy cảm này, hãy hủy nó. Dữ liệu bạn không có không thể bị đánh cắp.
- Không bao giờ lưu trữ thông tin thẻ tín dụng, nếu không muốn phải đối phó với việc tuân thủ PCI. Hãy đăng ký một bộ xử lý thanh toán như Stripe hoặc Braintree.
- Nếu bạn có dữ liệu nhạy cảm mà bạn thực sự cần, lưu trữ mã hóa nó và đảm bảo rằng tất cả các mật khẩu được sử dụng hàm Hash để bảo vệ. Đối với Hash, nên sử dụng bcrypt. Nếu bạn không sử dụng mã hoá bcrypt, hãy tìm hiểu về mã Salt để ngăn ngừa rainbow table attack.

Không lưu trữ các khóa mã hóa bên cạnh dữ liệu được bảo vệ. Việc này giống như khóa xe mà cấm chìa luôn ở đó. Bảo vệ bản sao lưu của bạn bằng mã hóa và đảm bảo các khóa của bạn là riêng tư.

2.2.7 Missing function level access control (lỗi phân quyền)

Đây chỉ là sai sót trong vấn đề phân quyền. Nó có nghĩa là khi một hàm được gọi trên máy chủ, quá trình phân quyền không chính xác. Các nhà phát triển dựa vào thực tế là phía máy chủ tạo ra giao diện người dùng và họ nghĩ rằng khách hàng không thể truy cập các chức năng nếu không được cung cấp bởi máy chủ.

Tuy nhiên, kẻ tấn công luôn có thể yêu cầu các chức năng “ẩn” và sẽ không bị cản trở bởi việc giao diện người dùng không cho phép thực hiện các chức năng này. Hãy tưởng tượng trong giao diện người dùng chỉ có bảng điều khiển/admin và nút nếu người dùng thực sự là quản trị viên. Không có gì ngăn cản kẻ tấn công phát hiện ra những tính năng này và lạm dụng nó nếu không phân quyền.

Cách ngăn chặn lỗ hổng:

Ở phía máy chủ, phải luôn được phân quyền một cách triệt để từ khâu thiết kế. Không có ngoại lệ – mọi lỗ hổng sẽ dẫn đến đủ các vấn đề nghiêm trọng.

2.2.8 Cross Site Request Forgery (CSRF)

Đây là một ví dụ của cuộc tấn công deputy attack. Trình duyệt bị đánh lừa bởi một số bên thứ ba lạm dụng quyền hạn. Ví dụ: trang web của bên thứ ba gửi yêu cầu đến trang web đích (ví dụ: ngân hàng của bạn) sử dụng trình duyệt của bạn với các dữ liệu như cookie và phiên người dùng. Nếu bạn đang đăng nhập vào một trang trên trang chủ của ngân hàng và trang đó dễ bị tấn công, một tab khác có thể cho phép kẻ tấn công đóng giả người quản trị. Deputy là khi trang web lạm dụng quyền hạn của mình (session cookies) để làm điều gì đó mà kẻ tấn công yêu cầu.

Cách ngăn chặn lỗ hổng:

Lưu trữ một Token bí mật trong một trường form ẩn mà không thể truy cập được từ trang web của bên thứ ba. Tất nhiên bạn phải xác minh trường ẩn này. Một số trang web yêu cầu mật khẩu của bạn cũng như khi sửa đổi các cài đặt nhạy cảm.

2.2.9 Using component with known vulnerabilities

Đây là vấn đề xảy ra khi sử dụng các bộ thư viện đã tồn tại lỗ hổng. Trước khi tích hợp một mã nguồn mới vào website, hãy thực hiện một số nghiên cứu hoặc kiểm tra bảo mật. Sử dụng mã nguồn mà bạn nhận được từ một người ngẫu nhiên trên GitHub hoặc một số diễn đàn có thể rất thuận tiện. Nhưng hãy sẵn sàng trước nguy cơ đối diện với một lỗ hổng bảo mật web nghiêm trọng.

Ví dụ: Nhiều trường hợp, trang admin bị lộ không phải vì các lập trình viên sai sót, mà vì phần mềm của bên thứ ba vẫn chưa được cập nhật. Nếu bạn nghĩ rằng họ sẽ không tìm thấy cài đặt phpmyadmin ẩn của bạn, hãy tìm hiểu về dirbuster.

Cách ngăn chặn lỗ hổng:

Chú ý cẩn thận khi sử dụng các thành phần của bên thứ 3, không nên là một coder copy-paste. Kiểm tra cẩn thận các đoạn code quan trọng của bạn. Nếu các đoạn code này có lỗ hổng, tin tặc có thể đọc cơ sở dữ liệu, tệp tin cấu hình, mật khẩu... của bạn.

Cập nhật mọi thứ: Đảm bảo bạn đang sử dụng phiên bản mới nhất của tất cả mọi thứ và có kế hoạch cập nhật chúng thường xuyên. Ít nhất là đăng ký bản tin về các lỗ hổng bảo mật mới liên quan đến sản phẩm.

2.2.10 Unvalidated redirects and forwards

Đây lại là vấn đề về lọc đầu vào. Giả sử rằng trang đích có một mô-đun redirect.php lấy URL làm tham số. Thao tác với tham số này có thể tạo ra một URL trên targetite.com chuyển hướng trình duyệt đến địa chỉ malwareinstall.com. Khi người dùng nhìn thấy liên kết, họ sẽ thấy liên kết targetite.com/blahblahblah tin cậy và truy cập vào. Họ ít biết rằng địa chỉ này thực ra chuyển tới trang nhúng phần mềm độc hại (hoặc bất kỳ trang độc hại khác). Ngoài ra, kẻ tấn công có thể chuyển hướng trình duyệt sang targetite.com/deleteprofile?confirm=1.

Cách ngăn chặn lỗ hổng:

- Không sử dụng chức năng chuyển hướng.
- Có một danh sách tĩnh các vị trí hợp lệ để chuyển hướng đến.
- Có Whitelist tham số người dùng xác định.

2.3 SEO đối với Website

SEO là gì?

SEO là từ viết tắt của “Search Engine Optimization” có nghĩa là “tối ưu hóa công cụ tìm kiếm”. Để website đạt được một thứ hạng nhất định trên công cụ tìm kiếm như Google, Bing, Yandex thì cần phải thực hiện cùng lúc các phương pháp nâng cao bao gồm SEO On-page và SEO Off-page. Đây là 2 quá trình luân phiên hỗ trợ lẫn nhau.

SEO On-page là gì?

Là phương pháp tối ưu hóa những gì hiển thị bên trong website của bạn như bố cục, hình ảnh, nội dung, video,.. nhằm mục đích tăng thứ hạng website trên công cụ tìm kiếm, cải thiện khả năng truy cập.

Nhiệm vụ của SEO On-page bao gồm:

- **Nghiên cứu từ khóa:** Công việc này giúp tăng lượt tìm kiếm và khớp hơn với nhu cầu của khách hàng. Đây cũng là bước đầu hỗ trợ đặt tiêu đề của bài viết hấp dẫn và thu hút hơn. Các công cụ nghiên cứu từ khóa mình hay dùng như Google Ads, ahrefs tool.
- **Tối ưu hóa bố cục bài viết:** Đó là những thẻ Heading, nên ưu tiên để từ khóa chính của bài viết xuất hiện ở các thẻ này, điều này sẽ giúp công cụ google tìm kiếm nhanh và duyệt bài của bạn nhanh hơn.
- **Tối ưu hình ảnh:** Chính là tối ưu thuộc tính tiêu đề hình ảnh giúp google nhận diện và đọc nội dung hình ảnh của bạn nhanh hơn, bên cạnh đó người dùng có thể tìm kiếm thông tin bạn đăng tải thông qua hình ảnh tốt hơn, tăng độ liên kết giữa bài viết và hình ảnh.

- **Tối ưu từ khóa:** Trong một bài viết google thường đánh giá cao những từ in đậm, chính vì vậy bạn cần in đậm tất cả cụm từ khóa chính và từ khóa liên quan để người đọc dễ dàng nhận thấy và tiếp thu nội dung chính mà bạn muốn truyền tải.
- **Tối ưu hóa link nội bộ:** Việc liên kết các bài viết trong một website có ảnh hưởng quan trọng đến sức mạnh chung của web, chính vì vậy cần xây dựng đường link dẫn trong bài viết kết nối với các bài viết khác trong cùng một website.
- **Tối ưu hóa nội dung:** Nếu những nhiệm vụ ở trên bạn đều làm rất tốt nhưng nội dung của bài viết kém hấp dẫn, thông tin không hữu ích với người đọc thì cũng vô ích. Đặc biệt là bài viết của bạn không được sao chép nguyên văn từ một bài viết khác có cùng nội dung, vì điều này sẽ làm google đánh giá kém và hạ thấp uy tín website của bạn.

SEO Off-page là gì?

Là phương pháp tối ưu hóa những gì hiển thị bên ngoài website của bạn bao gồm xây dựng liên kết (link building), marketing trên các kênh truyền thông: social media, social media bookmarking,... nhằm mục đích tăng số lượng liên kết có uy tín từ các trang web khác và google đánh giá đường link này như một phiếu tín nhiệm cho website của bạn.

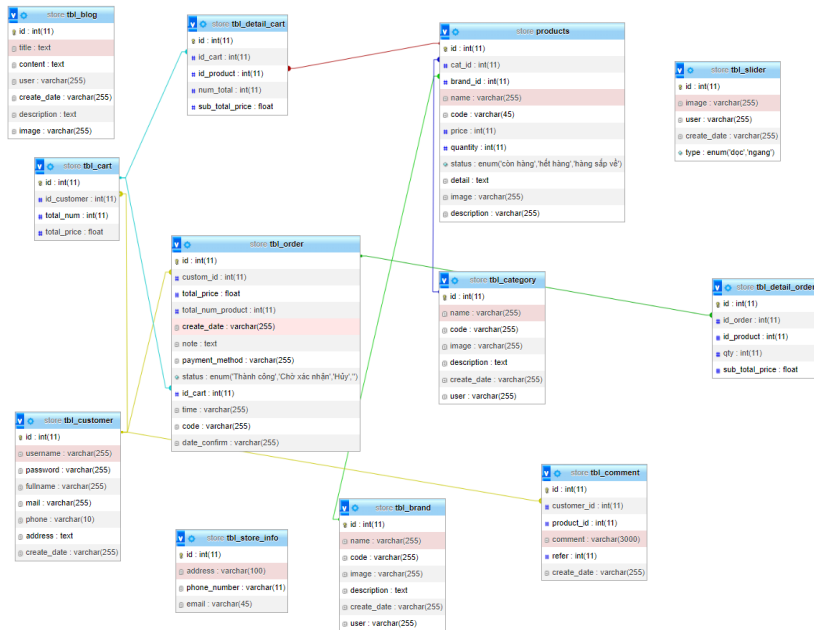
- **Tối ưu hóa link building:** Tức là tối ưu hóa backlink, việc liên kết với bài viết khác ngoài website đóng vai trò quan trọng, giúp chia sẻ 1 phần sức mạnh của trang web khác về trang web của mình. Google đánh giá sức mạnh của bạn dựa vào sức mạnh đường link dẫn từ website khác. Chính vì vậy việc lựa chọn website backlink phải hết sức thận trọng.
- **Social media:** là mạng xã hội như facebook, youtube, instagram, twitter, linked-in, foursquare, skype, yammer, flickr,... Tận dụng những đường link từ các trang mạng này trở về website của bạn là một cách nâng cao điểm số đánh giá của google, góp phần làm tăng sức mạnh của website.
- **Social media bookmarking:** là những trang mạng xã hội ít phổ biến hơn như reddit.com, stumbleupon.com, scoop.it, delicious.com. Bạn có thể dễ dàng tạo tài khoản tham gia và cũng là một cách giúp tăng lượt truy cập vào website của bạn.

Tại sao phải SEO?

SEO Website giúp website của bạn đứng đầu trang TOP của Google, làm tăng lượt truy cập vào website nhanh chóng hơn thông qua các công cụ tìm kiếm, từ đó làm tăng lợi nhuận cho doanh nghiệp, phân tích được lượng khách hàng tiềm năng, cải thiện uy tín và thương hiệu sản phẩm của doanh nghiệp.

3 Thiết Kế cơ sở dữ liệu








3.1 Mô hình thực thể liên kết









3.2 Quản trị viên (admin)

store tbl_admin	
admin_id	int(11)
username	varchar(255)
password	varchar(255)
fullname	varchar(255)
email	varchar(255)
phone	varchar(10)
address	varchar(255)
role	enum('admin','sale','manager')
create_date	timestamp

3.3 Bài viết

store tbl_blog	
	id : int(11)
	title : text
	content : text
	user : varchar(255)
	create_date : varchar(255)
	description : text
	image : varchar(255)

3.4 Thương hiệu

store tbl_brand	
	id : int(11)
	name : varchar(255)
	code : varchar(255)
	image : varchar(255)
	description : text
	create_date : varchar(255)
	user : varchar(255)


3.5 Giỏ hàng

v	store	tbl_cart
		id : int(11)
		# id_customer : int(11)
		# total_num : int(11)
		# total_price : float

3.6 Danh mục


v	store	tbl_category
		id : int(11)
		name : varchar(255)
		code : varchar(255)
		image : varchar(255)
		description : text
		create_date : varchar(255)
		user : varchar(255)

3.7 Khách hàng



store	tbl_customer
id	int(11)
username	varchar(255)
password	varchar(255)
fullname	varchar(255)
mail	varchar(255)
phone	varchar(10)
address	text
create_date	varchar(255)

3.8 Chi tiết giỏ hàng



store	tbl_detail_cart
id	int(11)
id_cart	int(11)
id_product	int(11)
num_total	int(11)
sub_total_price	float

3.9 Chi tiết đơn hàng

store	
tbl_detail_order	
id	int(11)
# id_order	int(11)
# id_product	int(11)
# qty	int(11)
# sub_total_price	float

3.10 Đơn hàng

store	
tbl_order	
id	int(11)
# custom_id	int(11)
# total_price	float
# total_num_product	int(11)
create_date	varchar(255)
note	text
payment_method	varchar(255)
status	enum('Thành công','Chờ xác nhận','Hủy','')
# id_cart	int(11)
time	varchar(255)
code	varchar(255)
date_confirm	varchar(255)

3.11 Sản phẩm

store products	
id : int(11)	
# cat_id : int(11)	
# brand_id : int(11)	
name : varchar(255)	
code : varchar(45)	
# price : int(11)	
# quantity : int(11)	
status : enum('còn hàng','hết hàng','hàng sắp về')	
detail : text	
image : varchar(255)	
description : varchar(255)	

3.12 Slider

store tbl_slider	
id : int(11)	
image : varchar(255)	
user : varchar(255)	
create_date : varchar(255)	
type : enum('dọc','ngang')	

3.13 Bình luận

store tbl_comment	
id : int(11)	
# customer_id : int(11)	
# product_id : int(11)	
comment : varchar(3000)	
# refer : int(11)	
create_date : varchar(255)	

3.14 Thông tin cửa hàng

store tbl_store_info	
id : int(11)	
address : varchar(100)	
phone_number : varchar(11)	
email : varchar(45)	

4 Hiện Thực

Source code on Github: [Click here](#)

5 Kết luận, hướng dẫn sử dụng và cài đặt

5.1 Kết luận

5.1.1 Những công việc đã làm được

- Thiết kế được mô hình cơ sở dữ liệu cho website.
- Thiết kế được giao diện người dùng khá trực quan và sinh động
- Ứng dụng được các kiến thức đã học về HTML, CSS, Bootstrap,... vào trang web
- Hiện thực được các function logic để ứng dụng vào việc hiện thị trang web

5.1.2 Hạn chế

- Do kinh nghiệm thực tế chưa có nhiều do vậy quá trình phân tích hệ thống cho website của cửa hàng còn nhiều chỗ chưa đúng với thực tế hay chưa đảm bảo tính đúng đắn. Vấn đề này nhóm em xin phép hoàn thiện thêm trong quá trình phát triển hệ thống sau đó.
- Giao diện trang web còn chưa thực sự đẹp mắt.
- Ngôn ngữ và phần mềm soạn thảo còn mới mẻ nên còn nhiều chức năng chưa tận dụng và kiểm soát được hết. Nhóm em rất mong được thầy Nguyễn Hữu Hiếu hỗ trợ để có thể hoàn thiện website một cách đầy đủ nhất.

5.1.3 Kết luận

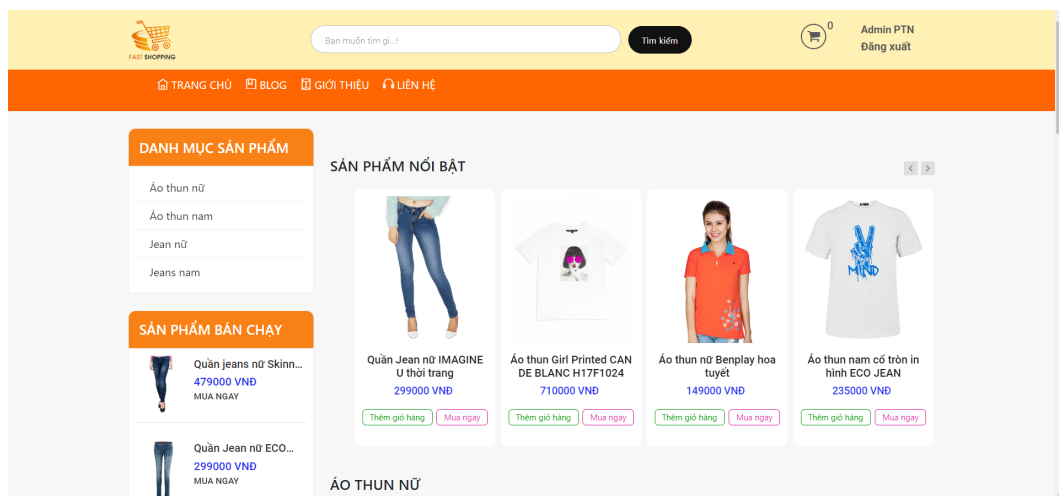
- Với sự nỗ lực của cả 3 thành viên trong nhóm nên đã tài đã được hoàn thành. Các yêu cầu của bài tập lớn cơ bản đã được đáp ứng tuy nhiên không thể tránh khỏi sai sót.

5.2 Hướng dẫn sử dụng và cài đặt

5.2.1 Hướng dẫn sử dụng

5.2.1.a Vào trang web

Giả sử http://localhost/web_programming/Source_code/?modules=home là đường link dẫn tới trang web, người dùng chỉ cần gõ link này vào thanh tìm kiếm trên trình duyệt thì website sẽ hiện lên:



5.2.1.b Tìm kiếm sản phẩm

Nếu bạn muốn tìm kiếm sản phẩm theo tên, hãy nhập tên sản phẩm vào ô tìm kiếm *Bạn muốn tìm gì...!* và nhấn vào nút tìm kiếm. Trang web sẽ chuyển bạn tới các sản phẩm theo yêu cầu.



Ngoài ra bạn cũng có thể sử dụng bộ lọc sản phẩm để lọc nhanh sản phẩm theo yêu cầu:

BỘ LỌC

Giá

- ☐ Dưới 100.000đ
- ☐ 100.000đ - 200.000đ
- ☐ 200.000đ - 400.000đ
- ☐ 400.000đ - 600.000đ
- ☐ Trên 600.000đ

Hãng

- ☐ CAN DE BLANC
- ☐ ALE JEANS
- ☐ Eco Jean
- ☐ IMAGINE U


Loại


- ☐ Jean nữ
- ☐ Jean name
- ☐ Áo thun nữ
- ☐ Áo thun nam

Áp dụng

5.2.1.c Đặt hàng

Để có thể đặt hàng trực tiếp trên trang web, bạn cần phải đăng nhập trước khi tiến hành đặt hàng. Nếu chưa có tài khoản, bạn có thể đăng kí.



 0 [Đăng nhập](#)
[Đăng kí](#)

[TRANG CHỦ](#) [BLOG](#) [GIỚI THIỆU](#) [LIÊN HỆ](#)

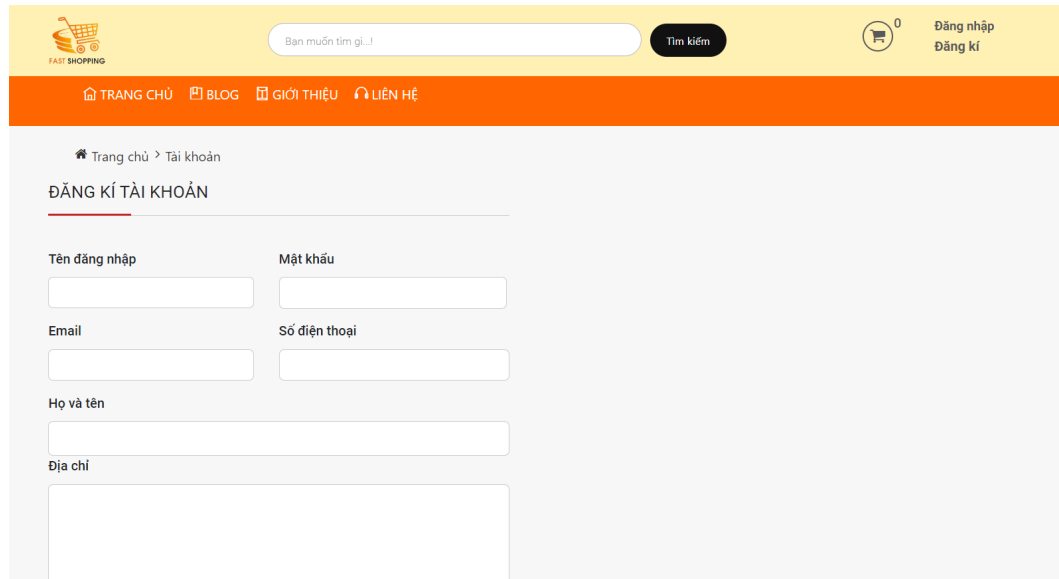
[Trang chủ](#) > [Tài khoản](#)

ĐĂNG NHẬP TÀI KHOẢN

Tên đăng nhập

Mật khẩu

[Đăng nhập với tư cách QTV](#)
[Hoặc đăng kí tài khoản tại đây](#)



FAST SHOPPING

Bạn muốn tìm gì...! [Tìm kiếm](#)

[0](#) [Đăng nhập](#) [Đăng ký](#)

[TRANG CHỦ](#) [BLOG](#) [GIỚI THIỆU](#) [LIÊN HỆ](#)

[Trang chủ](#) > [Tài khoản](#)

ĐĂNG KÍ TÀI KHOẢN

Tên đăng nhập

Mật khẩu

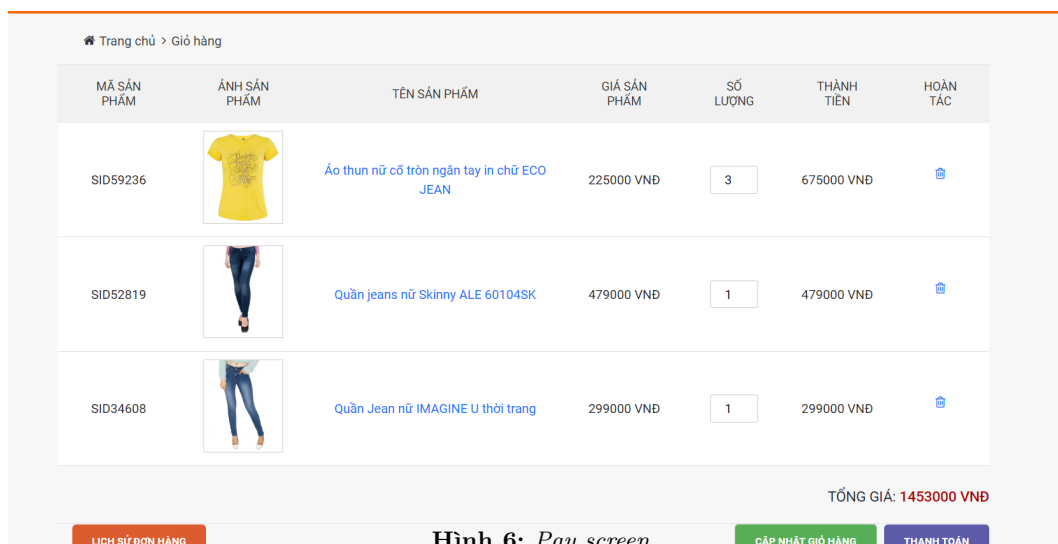
Email

Số điện thoại




Họ và tên

Địa chỉ

Lưu ý: khách hàng không được để trống thông tin đăng ký tài khoản. Sau khi đã đăng nhập hoặc đăng ký thì khách hàng đã có thể mua sản phẩm của mình mong muốn bằng cách bấm thêm vào giỏ hàng (nếu cần mua với số lượng nhiều) hoặc bấm vào mua ngay.



[Trang chủ](#) > [Giỏ hàng](#)

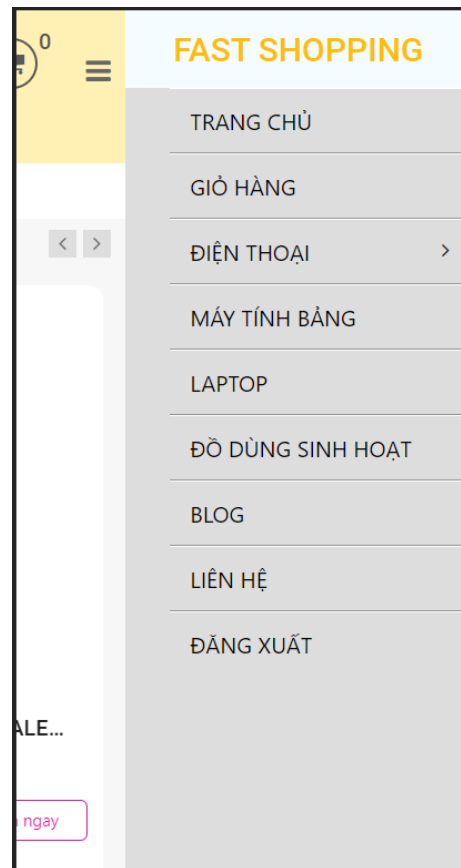
MÃ SẢN PHẨM	ẢNH SẢN PHẨM	TÊN SẢN PHẨM	GIÁ SẢN PHẨM	SỐ LƯỢNG	THÀNH TIỀN	HOÀN TÁC
SID59236		Áo thun nữ cổ tròn ngắn tay in chữ ECO JEAN	225000 VNĐ	<input type="text" value="3"/>	675000 VNĐ	Xóa
SID52819		Quần jeans nữ Skinny ALE 60104SK	479000 VNĐ	<input type="text" value="1"/>	479000 VNĐ	Xóa
SID34608		Quần Jean nữ IMAGINE U thời trang	299000 VNĐ	<input type="text" value="1"/>	299000 VNĐ	Xóa

TỔNG GIÁ: 1453000 VNĐ

[LỊCH SỬ ĐƠN HÀNG](#) [CẬP NHẬT GIỎ HÀNG](#) [THANH TOÁN](#)

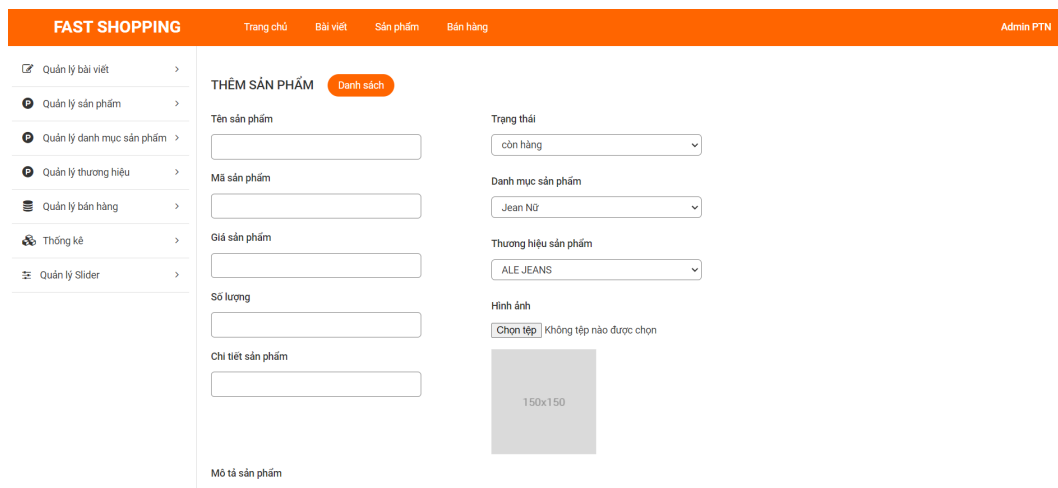
Hình 6: Pay screen

Ngoài ra nhóm chúng em có hiện thực reponsive design cho website:



5.2.1.d Các chức năng của quản trị viên

Bên cạnh đó, ta cũng có những chức năng cơ bản của **Admin**, dưới đây là chức năng thêm sản phẩm mới:



The image shows the 'FAST SHOPPING' Admin interface. The top navigation bar is orange and contains the text 'FAST SHOPPING' and 'Admin PTN'. Below the navigation bar, there is a sidebar with a list of management functions: 'Quản lý bài viết', 'Quản lý sản phẩm', 'Quản lý danh mục sản phẩm', 'Quản lý thương hiệu', 'Quản lý bán hàng', 'Thống kê', and 'Quản lý Slider'. The main content area is titled 'THÊM SẢN PHẨM' and includes a 'Danh sách' button. The form contains the following fields: 'Tên sản phẩm', 'Mã sản phẩm', 'Giá sản phẩm', 'Số lượng', 'Chi tiết sản phẩm', 'Mô tả sản phẩm', 'Trạng thái' (dropdown menu), 'Danh mục sản phẩm' (dropdown menu), 'Thương hiệu sản phẩm' (dropdown menu), and 'Hình ảnh' (image upload area with a 'Chọn tệp' button and a '150x150' placeholder).

Chức năng thêm, xoá, sửa danh mục sản phẩm:

FAST SHOPPING

Trang chủBản viếtSản phẩmBán hàngAdmin PTN

Quản lý bài viết

Quản lý sản phẩm

Quản lý danh mục sản phẩm

Quản lý thương hiệu

Quản lý bán hàng

Thống kê

Quản lý Slider





DANH MỤC SẢN PHẨM

Thêm mới

Tất cả (69) | Đã đăng (51) | Chờ xét duyệt(0) | Thùng rác(0)

Tác vụ

Áp dụng

<input type="checkbox"/>	STT	Mã danh mục	Hình ảnh	Danh mục	Người tạo	Thời gian	Hoàn tác
<input type="checkbox"/>	1	### Female Jean ###		Jean Nữ	admin	24/4/2023	<div><div></div><div></div></div>
<input type="checkbox"/>	2	### Female T-Shirt ###		Áo Thun Nữ	admin	24/4/2023	<div><div></div><div></div></div>
<input type="checkbox"/>	3	### Male T-Shirt ###		Áo Thun Nam	admin	25/4/2023	<div><div></div><div></div></div>
<input type="checkbox"/>	4	### Male Jeans ###		Jean Nam	admin	25/4/2023	<div><div></div><div></div></div>

Chức năng xử lý đơn hàng của khách hàng:

FAST SHOPPING

Trang chủBản viếtSản phẩmBán hàngAdmin PTN

Quản lý bài viết

Quản lý sản phẩm

Quản lý danh mục sản phẩm

Quản lý thương hiệu

Quản lý bán hàng

Thống kê

Quản lý Slider

DANH SÁCH ĐƠN HÀNG CẦN XỬ LÝ

Tất cả (69) | Đã đăng (51) | Chờ xét duyệt(0) | Thùng rác(0)

Tác vụ

Áp dụng

<input type="checkbox"/>	STT	Mã đơn hàng	Thời gian đặt	Khách hàng	Tổng số mặt hàng	Tổng tiền	Phương thức thanh toán	Hoàn tác
<input type="checkbox"/>	1	user(1670823317)	12/12/2022	phuc khanh	1	49990000	card_payment	xử lý
<input type="checkbox"/>	2	user(1670823343)	12/12/2022	phuc khanh	4	199960000	card_payment	xử lý

Chọn vào checkbox để lựa chọn tất cả

Và một số chức năng khác.

5.2.2 Hướng dẫn cài đặt

File database: store.sql

Cấu hình đường dẫn trong: admin/config/config.php (\$config['base_url'] = 'đường dẫn của máy hoặc đường dẫn host')

```
<?php
session_start();

/*
 * -----
 * BASE URL
 * -----
 * Cấu hình đường dẫn gốc của ứng dụng
 * Ví dụ:
 * http://hocweb123.com đường dẫn chạy online
 * http://localhost/yourproject.com đường dẫn dự án ở local
 *
 */

$config['base_url'] = "http://localhost/web_programming/Source_code/admin/";
//admin/modules/home
$config['default_module'] = 'home';
$config['default_controller'] = 'index';
$config['default_action'] = 'index';

|
```

Hình 7: Config

Cấu hình database trong: admin/config/database.php

```
<?php

/*
 * -----
 * CẤU HÌNH DATABASE
 * -----
 * Trong phần này chúng ta khai báo các thông số để cấu hình
 * Kết nối đến DB
 * -----
 * GIẢI THÍCH BIẾN
 * -----
 * hostname: Tên server
 * username: Tên đăng nhập kết nối
 * password: Mật khẩu kết nối
 * database: Tên database kết nối
 */

$db = array(
    'hostname' => 'localhost',
    'username' => 'root',
    'password' => '',
    'database' => 'store',
);
```

Hình 8: Config



Cấu hình đường dẫn ckeditor : admin/public/js/plugins/ckeditor
Cấu hình đường dẫn ckfinder: admin/public/js/plugins/ckfinder
Vào trang admin:
Đường dẫn vào trang quản trị /admin
Tài khoản admin : TK: admin , MK : admin
Tài khoản demo khách hàng : TK: taikhoan1, MK: 123456



Tài liệu

- [1] Top 10 lỗ hổng bảo mật Web phổ biến theo chuẩn OWASP – OWASP TOP 10 [Link](#)
- [2] SEO WEBSITE LÀ GÌ? TẠI SAO PHẢI SEO WEB [Link](#)
- [3] Bootstrap [Link](#)