

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC - KỸ THUẬT MÁY TÍNH



LẬP TRÌNH WEB (CO3049)

Assignment

THIẾT KẾ WEBSITE CHO CÔNG TY – DOANH NGHIỆP

Giảng viên hướng dẫn: Nguyễn Hữu Hiếu

Lớp: L07

Email: vu.le08@hcmut.edu.vn

Sinh viên: Nguyễn Thế Viễn - 1814764

Đào Thanh Tú - 1814656

Lê Tuấn Vũ - 1814812



Mục lục

1	Giới thiệu đề tài	4
2	Cơ sở lý thuyết	4
2.1	Reactjs	4
2.1.1	Ưu điểm	4
2.1.2	Nhược điểm	4
2.2	Bootstrap	5
2.2.1	Ưu điểm	5
2.2.2	Nhược điểm	5
2.3	Material UI	6
2.3.1	Ưu điểm	6
2.3.2	Nhược điểm	6
2.4	Slick	6
2.4.1	Ưu điểm	6
2.5	Font Awesome	7
2.5.1	Ưu điểm	7
2.6	XAMPP	7
2.6.1	Ưu điểm	8
2.6.2	Nhược điểm	8
2.6.3	Công cụ MySQL	8
2.7	SEO	9
2.7.1	Tối ưu On-Page	9
2.7.2	Tối ưu On-Page	9
2.8	Các lỗ hổng bảo mật trong ứng dụng web	10
2.8.1	Lỗ hổng Injection (Lỗi chèn mã độc)	10
2.8.2	Broken Authentication	10
2.8.3	Lỗ hổng XSS (Cross Site Scripting)	11
2.8.4	Insecure Direct Object References	11
2.8.5	Security Misconfiguration	11
2.8.6	Sensitive data exposure (Rò rỉ dữ liệu nhạy cảm)	12
2.8.7	Missing function level access control (lỗi phân quyền)	12
2.8.8	Cross Site Request Forgery (CSRF)	13



2.8.9 Using component with known vulnerabilities	13
2.8.10 Unvalidated redirects and forwards	13
3 Thiết kế ứng dụng	14
3.1 Thiết kế cơ sở dữ liệu	14
3.2 Thiết kế model ứng dụng	16
3.3 Cấu trúc mã nguồn	17
4 Tính năng và giao diện của ứng dụng	25
4.1 Các tính năng của khách hàng	25
4.1.1 Người dùng là khách	25
4.1.2 Người dùng là thành viên	25
4.2 Các tính năng của quản trị viên	25
4.2.1 Quản lý đơn hàng	25
4.2.2 Quản lý người dùng	26
4.2.3 Quản lý sản phẩm	26
4.2.4 Quản lý đánh giá, bình luận	27
4.3 Giao diện của ứng dụng	28
4.3.1 Màn hình Đăng nhập	28
4.3.2 Màn hình Đăng ký	28
4.3.3 Màn hình Trang chủ	29
4.3.4 Màn hình liên hệ	31
4.3.5 Màn hình tìm kiếm sản phẩm	32
4.3.6 Màn hình chính sách bảo mật	32
4.3.7 Màn hình giới thiệu	33
4.3.8 Màn hình trang hiển thị sản phẩm	35
4.3.9 Màn hình hiển thị chi tiết sản phẩm	37
4.3.10 Màn hình trang hiển thị thông số kỹ thuật sản phẩm	37
4.3.11 Màn hình trang hiển thị đánh giá, bình luận	38
4.3.12 Màn hình thông tin đặt hàng	38
4.3.13 Màn hình thay đổi thông tin cá nhân	39
4.3.14 Màn hình thay đổi mật khẩu	39
4.3.15 Màn hình admin quản lý đơn hàng	40
4.3.16 Màn hình admin quản lý tài khoản người dùng	40



4.3.17 Màn hình admin tạo tài khoản mới	41
4.3.18 Màn hình admin quản lý sản phẩm	41
4.3.19 Màn hình admin quản lý sản phẩm thêm thương hiệu	42
4.3.20 Màn hình admin quản lý thay đổi sản phẩm	42
4.3.21 Màn hình admin quản lý đánh giá, bình luận	43
5 Cách thức cài đặt ứng dụng	44
5.1 Yêu cầu hệ thống	44
5.2 Cách khởi động website	44
6 Đánh giá	45
6.1 Đánh giá kết quả đạt được	45
6.2 Hướng phát triển trong tương lai	45
6.3 Đánh giá mức độ thực hiện của các thành viên	45
Tài liệu tham khảo	46



1 Giới thiệu đề tài

Ngày nay, cùng với sự phát triển của internet, website đóng vai trò ngày càng quan trọng đối với việc quảng bá hình ảnh doanh nghiệp đến cộng đồng. Website đóng vai trò là kênh truyền thông, giới thiệu dịch vụ, sản phẩm, là công cụ kinh doanh mang lại những lợi thế cho một doanh nghiệp. Theo báo cáo năm 2019, tỉ lệ người dùng internet ở Việt Nam là 66%, và con số này sẽ ngày càng tăng trong tương lai. Chính vì vậy, việc sở hữu website đối với doanh nghiệp là vô cùng quan trọng, nhu cầu sở hữu website của các doanh nghiệp ngày càng lớn hơn.

Hiện thực website công ty - doanh nghiệp và sản phẩm cụ thể là các sản phẩm thiết bị điện tử như máy tính, điện thoại,... cho phép người dùng sử dụng nhiều tính năng như xem các trang thông tin như trang chủ, sản phẩm, thông tin liên hệ, ...

Hiện thực các tính năng quản lý website như quản lý đơn hàng, quản lý thông tin sản phẩm, quản lý người dùng, quản lý bình luận đánh giá của người dùng...

2 Cơ sở lý thuyết

2.1 Reactjs

Reactjs là một thư viện Javascript đang nổi lên trong những năm gần đây với xu hướng Single Page Application. Trong khi những framework khác cố gắng hướng đến một mô hình MVC hoàn thiện thì React nổi bật với sự đơn giản và dễ dàng phối hợp với những thư viện Javascript khác.

Nếu như AngularJS là một Framework cho phép nhúng code javascript trong code html thông qua các attribute như ng-model, ng-repeat... thì với react là một library cho phép nhúng code html trong code javascript nhờ vào JSX, bạn có thể dễ dàng lồng các đoạn HTML vào trong JS. Tích hợp giữa javascript và HTML vào trong JSX làm cho các component dễ hiểu hơn.

2.1.1 Ưu điểm

- Các component có thể tái sử dụng của React đảm bảo rằng các lập trình viên không phải viết đi viết lại cùng một đoạn code.
- Do tính phổ biến của react, việc tìm kiếm sự giúp đỡ, tài nguyên dành cho React là rất dễ dàng.

2.1.2 Nhược điểm

- Sự tập trung cao độ của React vào phát triển UI có thể khiến các khía cạnh khác trở nên khó khăn.
- Để học React bạn cần một nền tảng tốt, một phần do tài liệu không nhất quán.



2.2 Bootstrap

Bootstrap là sản phẩm của Mark Otto và Jacob Thornton tại Twitter. Nó được xuất bản như là một mã nguồn mở vào ngày 19/8/2011 trên GitHub. Tên gọi ban đầu là Twitter Blueprint. Bootstrap là một framework bao gồm các HTML, CSS và JavaScript template dùng để phát triển website chuẩn responsive.

Bootstrap bao gồm những cái cơ bản có sẵn như: typography, forms, buttons, tables, navigation, modals, image carousels và nhiều thứ khác. Trong bootstrap có thêm nhiều Component, Javascript hỗ trợ cho việc thiết kế responsive của bạn dễ dàng, thuận tiện và nhanh chóng hơn.

2.2.1 Ưu điểm

- **Dễ dàng thao tác:** cơ chế hoạt động của Bootstrap là dựa trên xu hướng mã nguồn mở HTML, CSS và Javascript. Người dùng cần trang bị kiến thức cơ bản 3 mã này mới có thể sử dụng Bootstrap hiệu quả. Bên cạnh đó, các mã nguồn này cũng có thể dễ dàng thay đổi và chỉnh sửa tùy ý.
- **Tuỳ chỉnh dễ dàng:** Bootstrap được tạo ra từ các mã nguồn mở cho phép designer linh hoạt hơn. Giờ đây có thể lựa chọn những thuộc tính, phần tử phù hợp với dự án họ đang theo đuổi. CDN Boostrap còn giúp bạn tiết kiệm dung lượng vì không cần tải mã nguồn về máy.
- **Chất lượng sản phẩm đầu ra hoàn hảo:** Bootstrap là sáng tạo của các lập trình viên giỏi trên khắp thế giới. Bootstrap đã được nghiên cứu và thử nghiệm trên các thiết bị. Được kiểm tra nhiều lần trước khi đưa vào sử dụng. Do đó, khi chọn Bootstrap, bạn có thể tin rằng mình sẽ tạo nên những sản phẩm với chất lượng tốt nhất.
- **Độ tương thích cao:** Điểm cộng lớn nhất của Bootstrap là khả năng tương thích với mọi trình duyệt và nền tảng. Đây là một điều cực kì quan trọng và cần thiết trong trải nghiệm người dùng. Sử dụng Grid System cùng với hai bộ tiền xử lý Less và Sass, Bootstrap mặc định hỗ trợ Responsive và ưu tiên cho các giao diện trên thiết bị di động hơn. Bootstrap có khả năng tự động điều chỉnh kích thước trang website theo khung browser. Mục đích để phù hợp với màn hình của máy tính để bàn, tablet hay laptop.

2.2.2 Nhược điểm

- **Tính kén phổ biến:** Bootstrap không phải là ứng dụng web phổ biến nên để tìm được một tổ chức, cá nhân thành thạo bootstrap để có thể sử dụng với nền tảng lập trình web không nhiều.
- **Sản phẩm nặng, tốc độ tối ưu chưa cao:** nên nếu dự án của bạn đòi hỏi sản phẩm nhẹ thì việc sử dụng bootstrap sẽ là cả một gánh nặng cho web.
- **Chưa hoàn thiện:** Bootstrap chưa đầy đủ các thư viện cần thiết. Các phát triển chưa thể tạo ra một framework riêng hoàn hảo, do đó một số trang web vẫn phải dùng phiên bản dành riêng cho mobile
- **Quá nhiều code thừa:** Không thể phủ nhận rằng Bootstrap có rất nhiều ưu điểm khi nó cũng 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.

- **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 trông cũng ổn ổn. Sự tiện dụng và dễ dàng của Bootstrap nhiều khi sẽ khuyến khích tính lười sáng tạo, vốn luôn thường trực trong mỗi chúng ta. Kết quả là, chúng ta thường thoả hiệp những gì mình thực sự muốn cho website để đổi lấy sự tiện dụng và tiết kiệm thời gian mà Bootstrap mang lại.

2.3 Material UI

Material UI là một thư viện các React Component đã được tích hợp thêm cả Google's Material Design. Theo như giới thiệu trên trang chủ thì được xây dựng nhờ React và Google's Material Design. Do đó phần hướng dẫn trên trang chủ của Material UI cũng nói nên sử dụng Material UI với React.

2.3.1 Ưu điểm

- Material UI đem đến cho bạn và trang web của bạn một giao diện hoàn toàn mới, với những button, textfield, toogle... được design theo một phong cách mới lạ, thay vì việc chỉ dùng Bootstrap như hiện nay.
- Cách dễ nhất để đáp ứng các nguyên tắc thiết kế material design của Google.
- Khả năng tùy biến cao.

2.3.2 Nhược điểm

- Không nhằm mục đích phục vụ như một điểm khởi đầu cho các dự án thiết kế web từ đầu.
- Cần hiểu rõ về React để sử dụng hiệu quả.

2.4 Slick

Slick là một thư viện javascript rất phổ biến dùng để tạo carousel một cách hiệu quả và dễ dàng tạo ra những responsive tuyệt đẹp.

2.4.1 Ưu điểm

- Slick tạo ra những responsive carousel tuyệt đẹp, tương thích với các màn hình khác nhau cũng như trình duyệt khác nhau, giúp tiết kiệm thời gian khởi tạo dự án.



2.5 Font Awesome

Font Awesome là một thư viện phông chữ và biểu tượng dựa trên CSS và LESS. Nó được tạo bởi Dave Gandy để sử dụng với Bootstrap và sau đó được tích hợp vào BootstrapCDN. Font Awesome chiếm 38% thị phần trong tổng số các website sử dụng Tập lệnh Phông chữ của bên thứ ba trên nền tảng của họ, xếp thứ hai sau Google Fonts.

2.5.1 Ưu điểm

- Một font chữ, 605 icons – đó là điều tuyệt vời nhất mà Font Awesome mang lại.
- Không bắt buộc JavaScript, chính vì thế mà bạn không cần phải lo lắng về tính tương thích của nó.
- Không cần phải lo lắng về việc chi phí đắt đỏ bởi vì nó hoàn toàn miễn phí cho tất cả các mục đích thương mại của bạn.
- Tương thích với cả Screen Reader – Font Awesome sẽ không bao giờ vượt qua bất kỳ trình đọc màn hình nào.
- Tính năng kiểm soát CSS – mọi thứ có thể có trong CSS đều được thực hiện dễ dàng và nhanh nhất có thể.
- Cung cấp khả năng mở rộng vô hạn – có một đồ họa vector có thể mở rộng chỉ ngụ ý rằng bất kỳ nếu biểu tượng chắc chắn sẽ trông tuyệt vời ở mọi kích thước.
- Font Awesome sử dụng linh hoạt giúp lập trình viên không mất quá nhiều thời gian để lấy các icons từ file PSD.

2.6 XAMPP

XAMPP là chương trình tạo web server được ứng dụng trên các hệ điều hành Linux, MacOS, Windows, Cross-platform, Solaris. XAMPP hoạt động dựa trên sự tích hợp của 5 phần mềm chính là Cross-Platform (X), Apache (A), MariaDB (M), PHP (P) và Perl (P), nên tên gọi XAMPP cũng là viết tắt từ chữ cái đầu của 5 phần mềm này:

- Chữ X đầu tiên là viết tắt của hệ điều hành mà nó hoạt động với: Linux, Windows và Mac OS X.
- **Apache:** Web Server mã nguồn mở Apache là máy chủ được sử dụng rộng rãi nhất trên toàn thế giới để phân phối nội dung Web. Ứng dụng được cung cấp dưới dạng phần mềm miễn phí bởi Apache Software Foundation.
- **MySQL / MariaDB:** Trong MySQL, XAMPP chứa một trong những hệ quản trị cơ sở dữ liệu quan hệ phổ biến nhất trên thế giới. Kết hợp với Web Server Apache và ngôn ngữ lập trình PHP, MySQL cung cấp khả năng lưu trữ dữ liệu cho các dịch vụ Web. Các phiên bản XAMPP hiện tại đã thay thế MySQL bằng MariaDB (một nhánh của dự án MySQL do cộng đồng phát triển, được thực hiện bởi các nhà phát triển ban đầu).



- **PHP:** Ngôn ngữ lập trình phía máy chủ PHP cho phép người dùng tạo các trang Web hoặc ứng dụng động. PHP có thể được cài đặt trên tất cả các nền tảng và hỗ trợ một số hệ thống cơ sở dữ liệu đa dạng.
- **Perl:** ngôn ngữ kịch bản Perl được sử dụng trong quản trị hệ thống, phát triển Web và lập trình mạng. Giống như PHP, Perl cũng cho phép người dùng lập trình các ứng dụng Web động.

2.6.1 Ưu điểm

- XAMPP có thể chạy được trên tất cả các hệ điều hành: Từ Cross-platform, Window, MacOS và Linux.
- XAMPP có cấu hình đơn giản cũng như nhiều chức năng hữu ích cho người dùng. Tiêu biểu gồm: giả lập Server, giả lập Mail Server, hỗ trợ SSL trên Localhost.
- Mã nguồn mở: Không như Appserv, XAMPP có giao diện quản lý khá tiện lợi. Nhờ đó, người dùng có thể chủ động bật tắt hoặc khởi động lại các dịch vụ máy chủ bất kỳ lúc nào.

2.6.2 Nhược điểm

- Tuy nhiên do cấu hình đơn giản nên XAMPP không được hỗ trợ cấu hình Module nên cũng không có Version MySQL. Do đó đôi khi sẽ mang đến sự bất tiện cho từng người. Trong khi WAMP có nhiều tùy chọn hơn vì nó có nhiều phiên bản cho từng thành phần của server như PHP, Apache, MySQL.
- Dung lượng của XAMPP cũng tương đối nặng, dung lượng file cài đặt của XAMPP là 141Mb, nặng hơn nhiều so với WAMP chỉ 41Mb.

2.6.3 Công cụ MySQL

MySQL là một trong những trình quản lý cơ sở dữ liệu thông dụng nhất hiện nay trong phiên bản php 5.0 trở về trước mysql không còn được hỗ trợ. Mysql có hai cách kết nối cơ sở liệu: kết nối bằng hàm, bằng hướng đối tượng. Các bước thao tác trên cơ sở dữ liệu:

- Bước 1: Tạo kết nối.
- Bước 2: Mở kết nối dữ liệu.
- Bước 3: Tạo lệnh điều khiển truy vấn SQL.
- Bước 4: Thực thi lệnh.
- Bước 5: Đóng kết nối.
- Bước 6: In kết quả.



2.7 SEO

Google sử dụng PageRank để xác định độ quan trọng của một trang web được đo trên thang điểm 10. PageRank là một trong các nhân tố chính để có được vị trí cao trong SERP (Search Engine Results Page). Điểm mấu chốt để có được xếp hạng cao là làm cho trang web có được các nhân tố phù hợp với giải thuật của công cụ tìm kiếm sử dụng để xử lý xếp hạng.

SEO là từ viết tắt của Search Engine Optimization (tối ưu hóa công cụ tìm kiếm), là một quy trình nâng cao thứ hạng của website trên các công cụ tìm kiếm giúp người dùng có thể tìm thấy trang web dễ dàng hơn trên bảng kết quả tìm kiếm. Trong bảng kết quả tìm kiếm thì SEO đứng dưới các vị trí của quảng cáo Adwords (hiện tại các kết quả Adword sẽ có chữ “Quảng cáo” xuất hiện trên mẩu quảng cáo). Các kết quả SEO có được sau 1 quá trình nỗ lực tối ưu và đạt được các thứ hạng phổ biến thường được gọi từ TOP 1 đến TOP 10 (vị trí số 1 đến vị trí số 10 trên 1 trang).

2.7.1 Tối ưu On-Page

- **Tối ưu title và meta tag:** Những tag sẽ giúp các công cụ tìm kiếm có được các thông tin phù hợp mô tả nội dung của trang web giúp các công cụ xác định được trang web đó có phù hợp trong danh sách kết quả trả về phản hồi trong một lần yêu cầu tìm kiếm. Những meta tag quan trọng nhất là title tag, meta description (hiển thị trên SERP 160 ký tự), keywords tag. Bên cạnh đó header tags cũng là một nhân tố SEO quan trọng bởi vì công cụ tìm kiếm sẽ đánh giá cao nó hơn những phần khác để xác định nội dung của trang web và các phần nội dung của trang đó.
- **Tối ưu nội dung trang web:** nội dung là thứ công cụ tìm kiếm cần để liên kết trang web với tập các từ khóa và những cụm từ khóa.
- **Tạo file sitemap:** file sitemap là một trang xml trên website. Nó chứa các đường link đến những trang web của một website và chi tiết của phân cấp của những trang đó. Cung cấp file sitemap sẽ giúp công cụ tìm kiếm của Google index trang được dễ dàng hơn và không bị bỏ sót trang.
- **Tối ưu liên kết ảnh và ảnh:** Tối ưu ảnh sẽ giúp công cụ tìm kiếm hiểu thông tin ảnh của trang web mô tả hơn. Từ đó nó sẽ giúp công cụ tìm kiếm dễ dàng crawl và xếp hạng ảnh đó cao hơn. Có một vài cách để tối ưu ảnh gồm: ảnh chất lượng cao và phù hợp với nội dung trang web, dùng những keyword trong file ảnh, dùng các text có nội dung mô tả trong thuộc tính alt, tạo ra các file ảnh có kích thước khác nhau thay vì scale ảnh.
- **Tạo và tối ưu file robot.txt:** file robot.txt sẽ giúp bổ sung cho file sitemap hỗ trợ cho crawler của công cụ tìm kiếm với những hướng dẫn đọc và index website, cụ thể là các trang được index và các trang nên bỏ qua vì những thông tin riêng tư cần bảo vệ.

2.7.2 Tối ưu Off-Page

Tối ưu Off-Page là tất cả những thứ giúp gia tăng độ tin cậy và uy tín của website. Nó được xác định bởi số lượng, chất lượng và độ phù hợp của các liên kết đến website. Điều đó tạo nên SEO authority và ảnh hưởng đến xếp hạng của kết quả tìm kiếm.

Những cách để tối ưu Off-Page:



- Xây dựng các liên kết từ các website khác liên kết đến website của bạn. Công cụ tìm kiếm sẽ dựa trên số lượng và chất lượng của liên kết đến website của bạn.
- Tạo ra các nội dung duy nhất, phù hợp trên những liên kết đến website của bạn sẽ thu được nhiều sự chú ý và nhanh chóng phổ biến hơn.
- Mạng xã hội là một nền tảng tốt giúp kết nối và có các cuộc hội thoại thật với những khán giả của bạn. Thường xuyên đăng những bài viết có chất lượng và sáng tạo sẽ thu hút được nhiều sự quan tâm sẽ tạo ra các tín hiệu tốt trên mạng xã hội với công cụ tìm kiếm từ đó sẽ nâng cao xếp hạng một cách tự nhiên.
- Press Release luôn được các công cụ tìm kiếm ghi nhận và index. Đó là một nhân tố xếp hạng của công cụ tìm kiếm và nâng cáo độ tin cậy cho website của bạn.

2.8 Các lỗ hổng bảo mật trong ứng dụng web

2.8.1 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 lỗ lọt dữ liệu và chiếm quyền kiểm soát trình duyệt của khách hàng.

Cách ngăn chặn lỗ hổng:

- Để chống lại lỗ hổng này cần lọc đầu vào đúng cách chưa hay việc bạn cần 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.
- 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.

2.8.2 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.

2.8.3 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>.

2.8.4 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.

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 kỳ 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.

2.8.5 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.

2.8.6 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 hóa 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 cắm chìa luôn ở đó. Bảo vệ bản sao lưu của bạn bằng mã hóa và đảm bảo các khóa của bạn là riêng tư.

2.8.7 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.

2.8.8 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.

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.

2.8.9 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.

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 tức có thể đọc cơ sở dữ liệu, tệp tin cấu hình, mật khẩu... của bạn. 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 đến sản phẩm.

2.8.10 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.

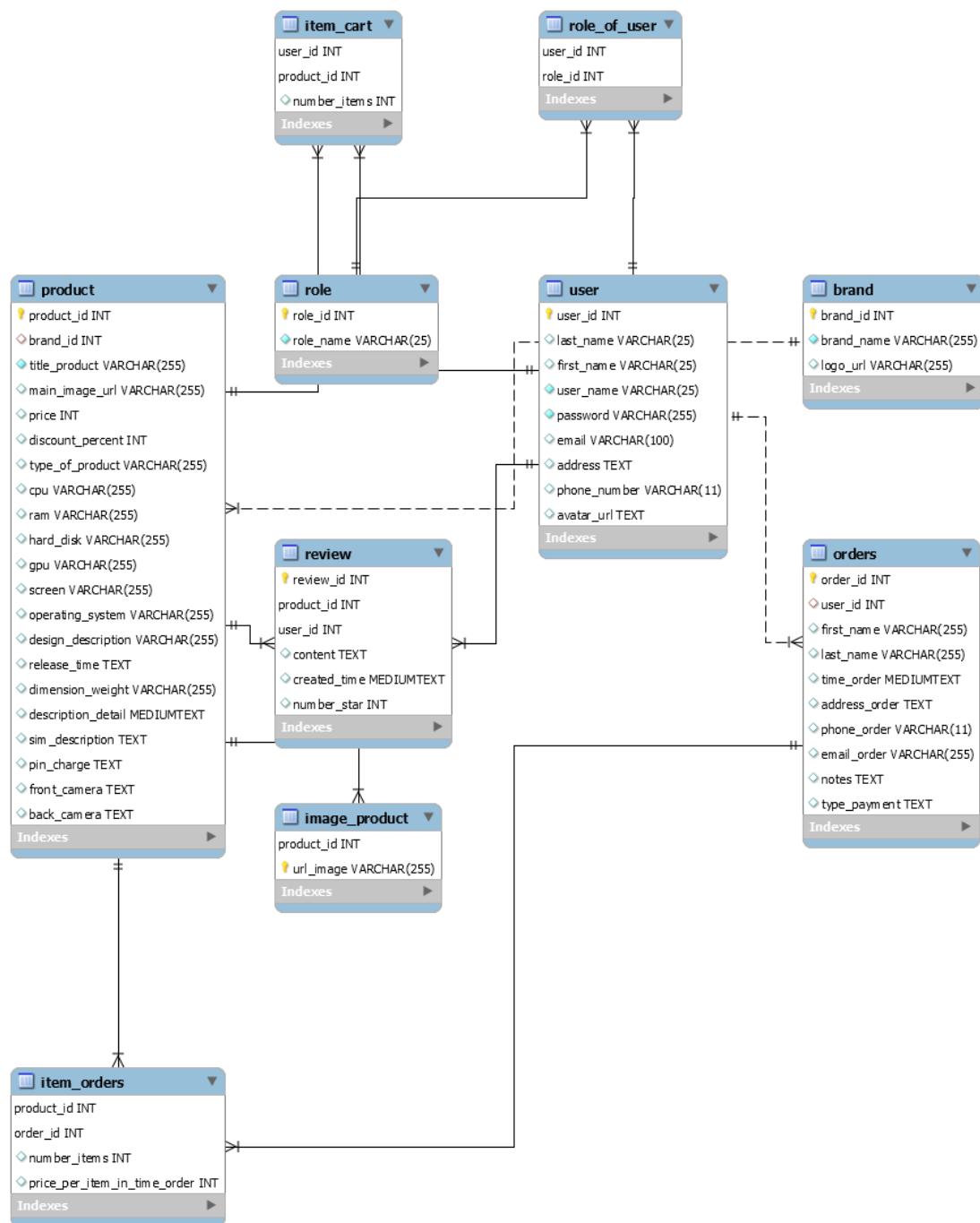
Cách ngăn chặn lỗ hổng:

- 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.



3 Thiết kế ứng dụng

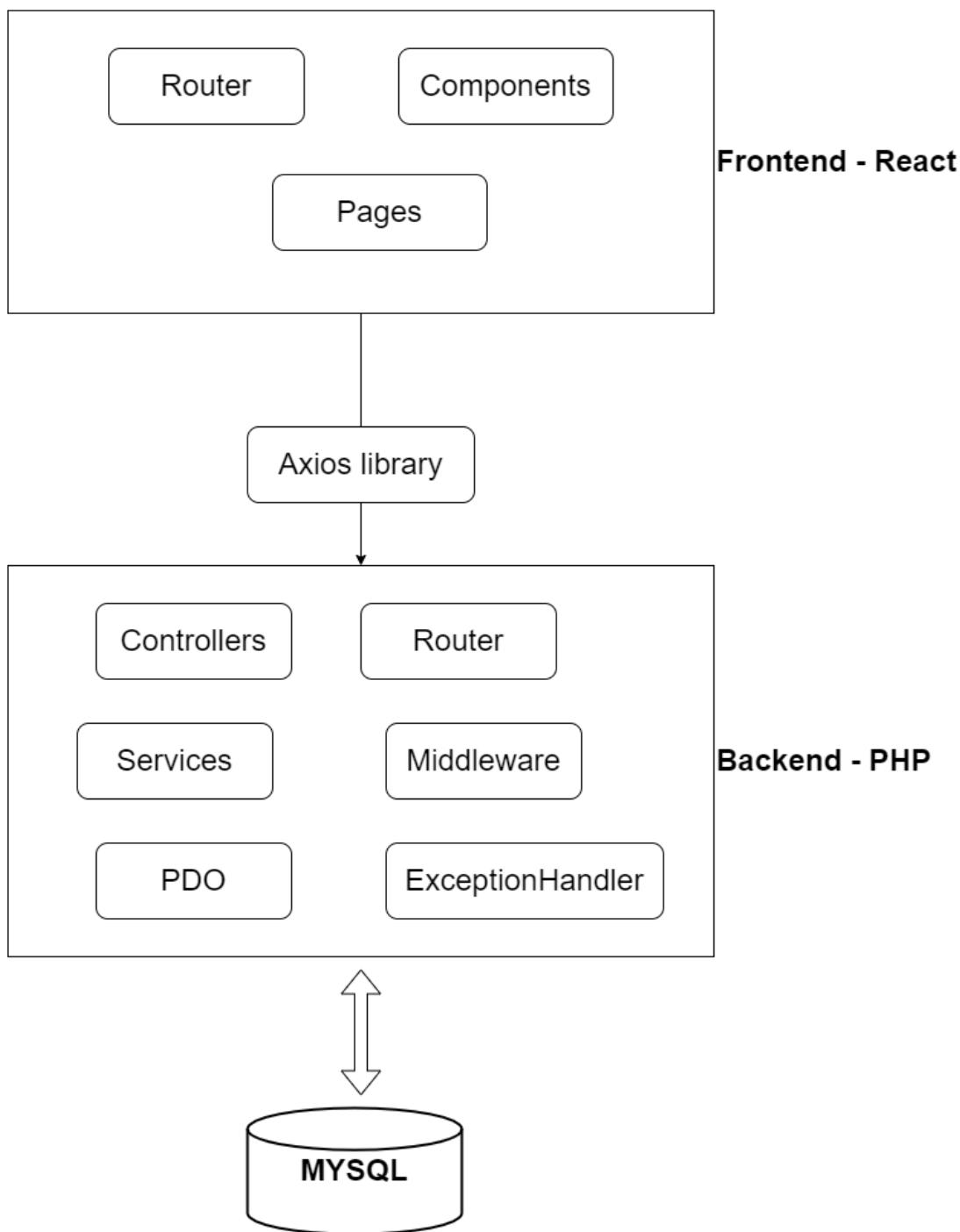
3.1 Thiết kế cơ sở dữ liệu





- product: Dữ liệu chính của ứng dụng là product gồm hai loại laptop và smartphone phân loại bằng thuộc tính type_of_product và có thuộc tính brand_id chỉ brand sản xuất product đó.
- brand: Thông tin brand sản xuất product.
- user: Thông tin của các thành viên và các admin của ứng dụng.
- role: Các role có trong ứng dụng.
- role_of_user: Mỗi quan hệ giữa user và role chỉ ra các role hiện có của user.
- item_cart: Các product mà user đã chọn vô cart gồm product_id để chỉ product và user_id để chỉ user.
- image_product: Các image của một product có product_id để chỉ product
- orders: Các order mà user đã thực hiện mua.
- item_orders: Các item của một order, item là các product với product_id để xác định product đó và order_id để chỉ order.
- review: Các bình luận và đánh giá của user về một product.

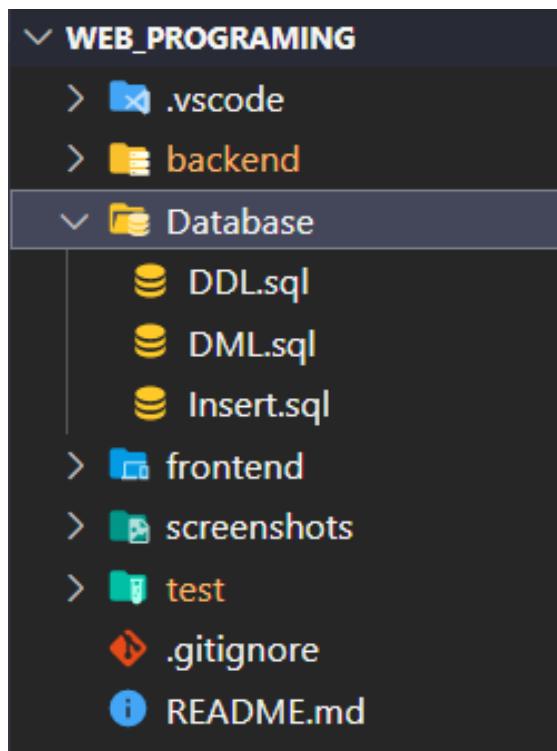
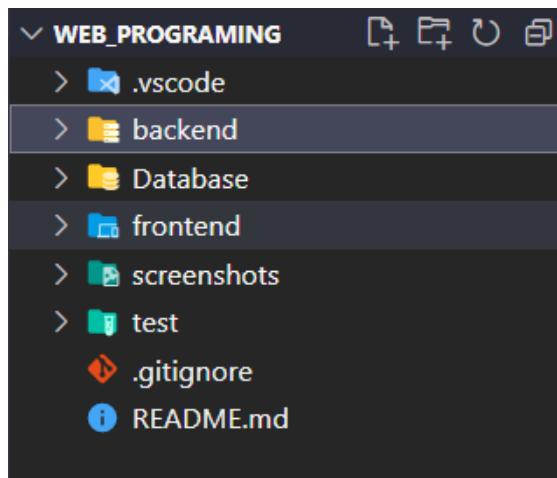
3.2 Thiết kế model ứng dụng



Hình 1: Model ứng dụng



3.3 Cấu trúc mã nguồn





The image shows two side-by-side file explorer windows, both titled "WEB PROGRAMMING".

Left File Explorer:

- Root: WEB PROGRAMMING
 - .vscode
 - backend
 - .idea
 - public
 - index.php
 - src
 - authentication
 - UserAuth.php
 - config
 - constants
 - HTTP.php
 - MessageHttpException.php
 - Role.php
 - Route.php
 - controllers
 - CommunityController.php
 - FileController.php
 - OrdersController.php
 - ProductController.php
 - UserController.php
 - core
 - ddd
 - mysqldb
 - route
 - util
 - vendor
 - .env
 - .env.example
 - .gitignore
 - bootstrap.php
 - composer.json

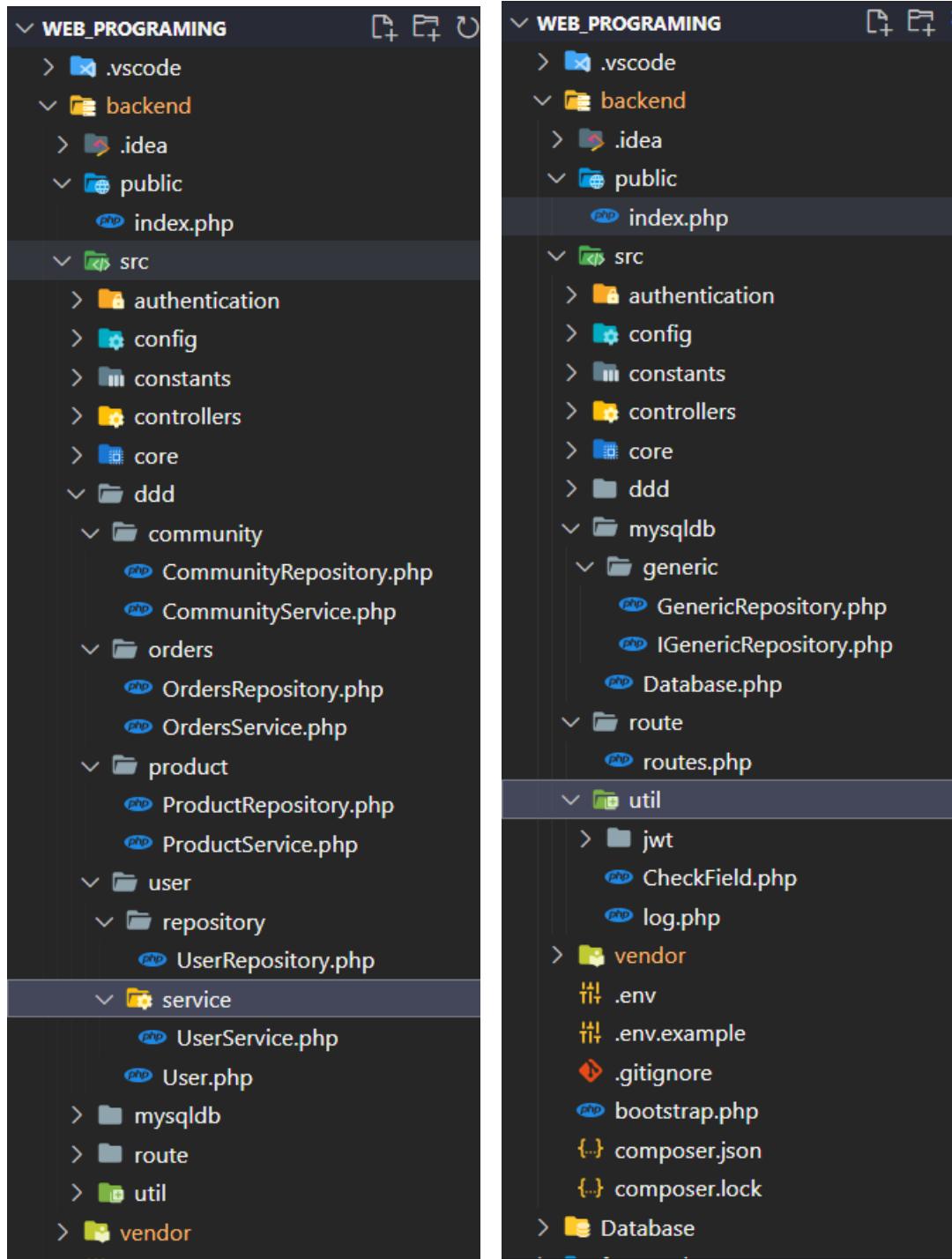
The image shows two side-by-side file explorer windows, both titled "WEB PROGRAMMING".

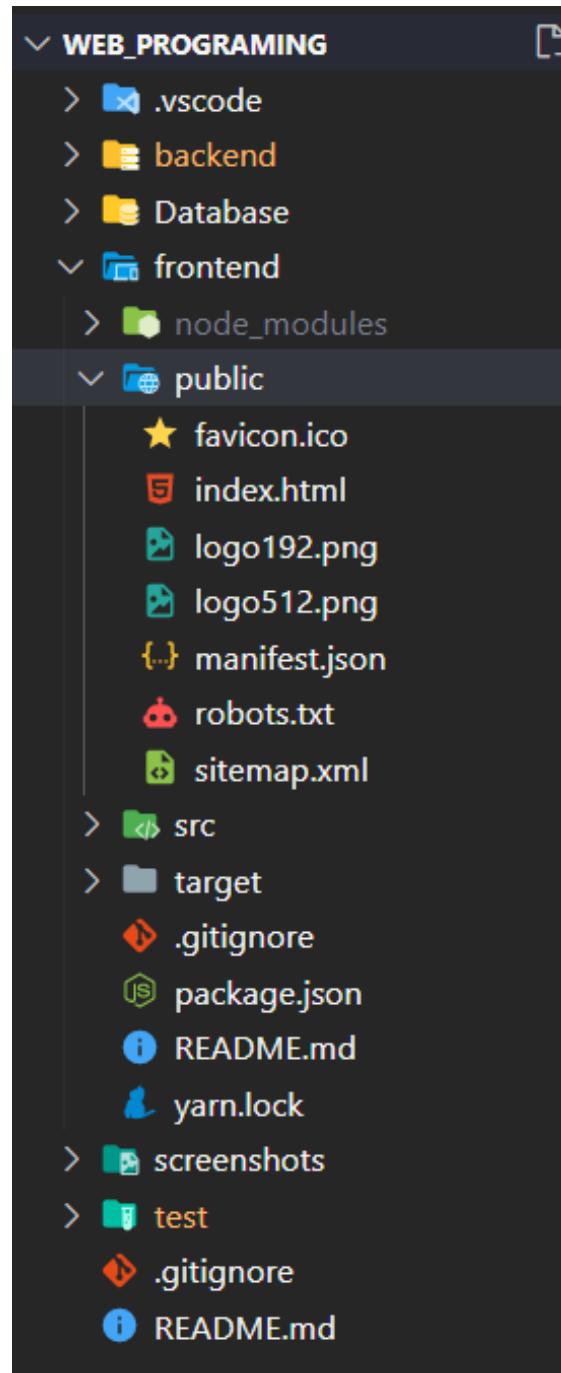
Right File Explorer:

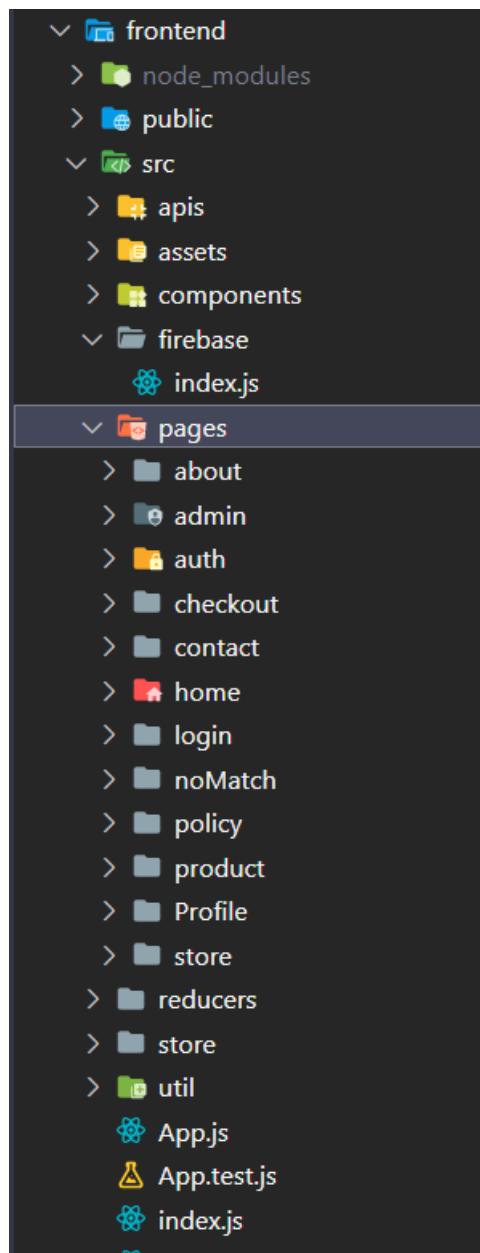
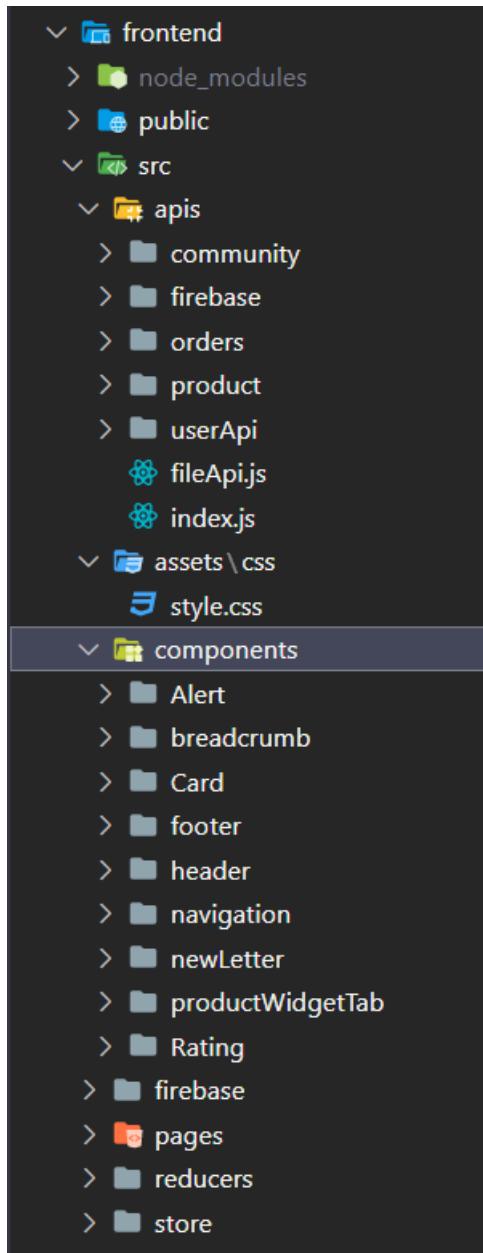
- Root: WEB PROGRAMMING
 - .vscode
 - backend
 - .idea
 - public
 - index.php
 - src
 - authentication
 - config
 - constants
 - controllers
 - core\http
 - Exception
 - HttpException.php
 - handler
 - RequestHandler.php
 - RequestHandlerInterface.php
 - httpMessage
 - HttpRequest.php
 - HttpRequestInterface.php
 - HttpResponse.php
 - HttpResponseInterface.php
 - middleware
 - MiddlewareAuthentication.php
 - MiddlewareController.php
 - MiddlewareHandleException.php
 - MiddlewareInterface.php
 - Route
 - ddd
 - mysqldb
 - route
 - util



- authentication: chứa model User authentication.
- constants: chứa các String static.
- controller: chứa tất cả các controller xử lý các request.
- core: chứa các phần logic xử lý request http gồm: maping url, các middleware, model httpException.
- ddd(domain drive design): nơi chứa toàn bộ domain, service, repository ở backend.
- mysqlDb: tạo connect tới mysql.
- route: định nghĩa các url, xác định permission, cũng như chỉ định các controller xử lý các request.









The image shows two side-by-side file explorer windows, likely from a code editor like VS Code. Both windows display the same directory structure for a 'frontend' project.

Left File Explorer:

- frontend
 - node_modules
 - public
 - src
 - apis
 - assets
 - components
 - firebase
 - index.js
 - pages
 - reducers
 - admin
 - productDetailReducer.js
 - customers
 - CartReducer.js
 - FilterProductReducer.js
 - productDetailReducer.js
 - triggerElement.js
 - UserInfo.js
 - home
 - FilterTypeProductReducer.js
 - AuthReducer.js
 - store
 - store.js
 - util
 - App.js
 - App.test.js
 - index.js

The image shows two side-by-side file explorer windows, likely from a code editor like VS Code. Both windows display the same directory structure for a 'frontend' project.

Right File Explorer:

- frontend
 - node_modules
 - public
 - src
 - apis
 - assets
 - components
 - firebase
 - pages
 - reducers
 - store
 - util
 - enum
 - storageKeys.js
 - orders
 - columnOrders.js
 - products
 - ColumTable.js
 - typeProduct.js
 - reviews
 - columnTable.js
 - string_utils
 - StringContent.js
 - users
 - columnTable.js
 - Roles.js
 - env.js
 - getCookie.js



- apis: sử dụng axios để thực hiện gửi request tới server.
- assets: chứa các file static như: images, css(global)...
- components: chứa các component được dùng chung trên toàn project.
- pages: nơi hiển thị các page của trang web như : home, admin, store, mỗi page sẽ chứa các components và css dùng cho page đó.
- reducers: sử dụng redux-toolkit để tạo các reducer dùng trong project.
- store: khởi tạo store và khai báo các reducer.
- util: chứa constants, env, cũng như các function tái sử dụng.



4 Tính năng và giao diện của ứng dụng

4.1 Các tính năng của khách hàng

4.1.1 Người dùng là khách

- Xem thông tin public trên trang web.
- Đăng ký người dùng mới: Đăng ký với tên đăng nhập và mật khẩu mà khách hàng đăng ký.

4.1.2 Người dùng là thành viên

- Đăng nhập: Đăng nhập với tên đăng nhập và mật khẩu đã đăng ký.
- Xem thông tin trên các trang: trang chủ, trang cửa hàng chứa sản phẩm, trang liên hệ, trang giới thiệu, trang chính sách bảo mật,...
- Tìm kiếm sản phẩm khách hàng muốn mua.
- Đặt hàng và thanh toán hóa đơn: Sau khi chọn sản phẩm muốn mua thì sẽ có một hóa đơn hiển thị thông tin khách hàng và sản phẩm mua cho khách hàng để xác nhận đặt hàng.
- Bình luận và đánh giá sản phẩm: Khách hàng có thể đánh giá sao và viết bình luận cho sản phẩm trên trang web.
- Thay đổi thông tin cá nhân, hình ảnh đại diện: Khách hàng có thể thay đổi thông tin cá nhân và hình đại diện của tài khoản sau khi tài khoản đã được xác minh.
- Thay đổi mật khẩu: Khách hàng có thể thay đổi mật khẩu hiện tại của tài khoản.

4.2 Các tính năng của quản trị viên

4.2.1 Quản lý đơn hàng

Tính năng:

- Xem thông tin đơn hàng.
- Sửa thông tin đơn hàng.
- Xóa thông tin đơn hàng.

Các thành phần trong trang gồm:

- **Thông tin bảng:**

- Hiển thị thông tin đơn hàng như ID đơn hàng, ID khách hàng, địa chỉ, email, số điện thoại, ...



- **Checkbox:** chọn để đánh dấu ID dùng cho việc xóa đơn hàng trên **database**, có tính năng chọn tất cả đơn hàng trên **Checkbox** của **heading**.

- **Nút xóa:**

- Kiểm tra tất cả các đơn hàng đã được đánh dấu bằng **Checkbox** để xóa thông tin đơn hàng của người dùng.

4.2.2 Quản lý người dùng

Tính năng:

- Xem thông tin người dùng.
- Tạo mới tài khoản.
- Sửa thông tin người dùng.
- Xóa thông tin người dùng.

Các thành phần trong trang gồm:

- **Thông tin bảng:**

- Hiển thị thông tin người dùng như ID, tên đăng nhập, email, số điện thoại, ...
- **Checkbox:** chọn để đánh dấu ID dùng cho việc xóa người dùng trên **database**, có tính năng chọn tất cả người dùng trên **Checkbox** của **heading**.

- **Nút xóa:**

- Kiểm tra tất cả các người dùng đã được đánh dấu bằng **Checkbox** để xóa thông tin đăng nhập của người dùng.

- **Nút tạo tài khoản mới:**

- Admin có thể tạo tài khoản mới gồm tên đăng nhập, mật khẩu và vai trò của người dùng.

4.2.3 Quản lý sản phẩm

Tính năng:

- Xem thông tin sản phẩm.
- Thêm thương hiệu.
- Thêm sản phẩm.
- Sửa sản phẩm.
- Xóa sản phẩm.



Các thành phần trong trang gồm:

- **Thông tin bảng:**

- Hiển thị thông tin sản phẩm như ID sản phẩm, tên sản phẩm, tên thương hiệu, giá tiền, năm phát hành, ...
- **Checkbox:** chọn để đánh dấu ID sản phẩm dùng cho việc xóa sản phẩm trên **database**, có tính năng chọn tất cả sản phẩm trên **Checkbox** của **heading**.

- **Nút xóa:**

- Kiểm tra tất cả các sản phẩm đã được đánh dấu bằng **Checkbox** để xóa thông tin sản phẩm.

- **Nút thêm thương hiệu:**

- Admin có thể thêm thương hiệu gồm tên thương hiệu và logo thương hiệu.

- **Nút thêm sản phẩm:**

- Admin có thể thêm sản phẩm gồm tên sản phẩm, tên thương hiệu, giá tiền, năm phát hành, mô tả chi tiết sản phẩm, ...

4.2.4 Quản lý đánh giá, bình luận

Tính năng:

- Xem thông tin đánh giá, bình luận.
- Xóa thông tin đánh giá, bình luận spam.

Các thành phần trong trang gồm:

- **Thông tin bảng:**

- Hiển thị thông tin đánh giá, bình luận như ID bình luận, ID khách hàng, ID sản phẩm, nội dung bình luận, ...
- **Checkbox:** chọn để đánh dấu ID dùng cho việc xóa bình luận trên **database**, có tính năng chọn tất cả bình luận trên **Checkbox** của **heading**.

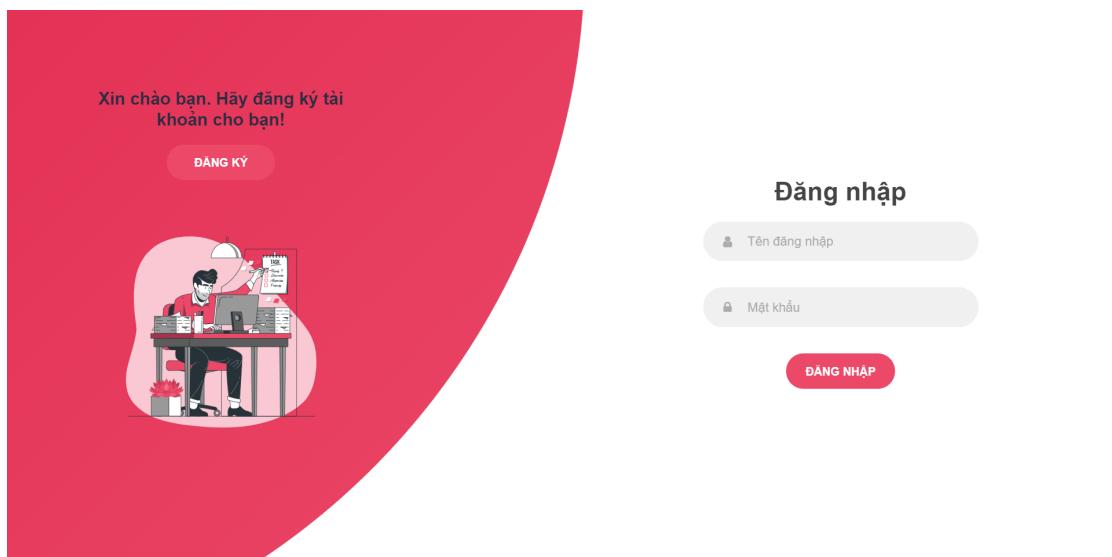
- **Nút xóa:**

- Kiểm tra tất cả các bình luận đã được đánh dấu bằng **Checkbox** để xóa nội dung bình luận của người dùng.



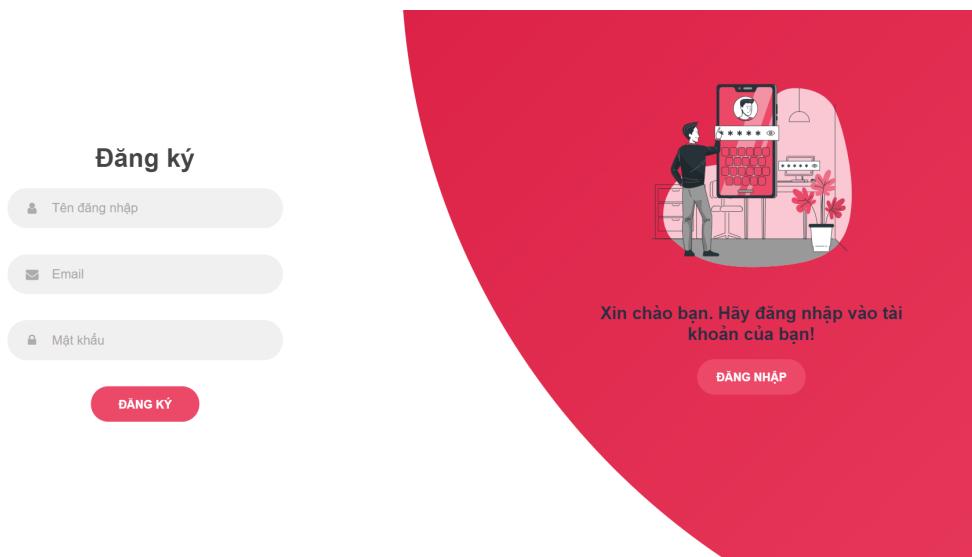
4.3 Giao diện của ứng dụng

4.3.1 Màn hình Đăng nhập



Hình 2: Màn hình đăng nhập

4.3.2 Màn hình Đăng ký



Hình 3: Màn hình đăng ký



4.3.3 Màn hình Trang chủ

The screenshot shows the homepage of BK COMPUTER. At the top, there is a dark header with contact information (0919523753, vu.le08@hcmut.edu.vn, KTX khu A, Đại học Quốc gia TP HCM), a login link ('Đăng xuất'), a 'Tài khoản' dropdown, and a shopping cart icon with '0' items. Below the header is the BK COMPUTER logo and a search bar. The main menu includes 'Trang chủ', 'Cửa hàng', 'Giới thiệu', 'Liên hệ', and 'Chính sách bảo mật'. Two large promotional banners are displayed: one for 'Bộ sưu tập Laptop' featuring a black laptop, and another for 'Bộ sưu tập Smartphone' featuring a silver smartphone. Below these banners, there are sections for 'SẢN PHẨM MỚI' (New Products) under 'LAPTOP' and 'SMARTPHONE' categories.

Hình 4: Màn hình trang chủ

This screenshot shows a grid of new products on the BK COMPUTER website. It includes four smartphone models: REALME 7 PRO, REALME 8, SAMSUNG GALAXY A52S 5G, and a laptop, the ASUS ZENBOOK FLI. Each product card displays the device's image, name, price, and a star rating. The laptop card also lists its specifications: Intel Core i5-1135G7, 16GB RAM, 512GB SSD, 13.3" FullHD screen, and a starting price of \$1103.

Hình 5: Màn hình trang chủ hiển thị sản phẩm mới



The banner features a laptop on the left and a pair of headphones on the right. In the center, four red circles show a timer: 02 NGÀY, 10 GIỜ, 34 PHÚT, and 60 GIÂY. Below the timer, the text reads "GIÁ SÓC TUẦN NÀY" and "BỘ SƯU TẬP MỚI GIẢM GIÁ TỚI 50%". A red button at the bottom says "MUA HÀNG NAY BÂY GIỜ!".

CHƯƠNG TRÌNH KHUYẾN MÃI

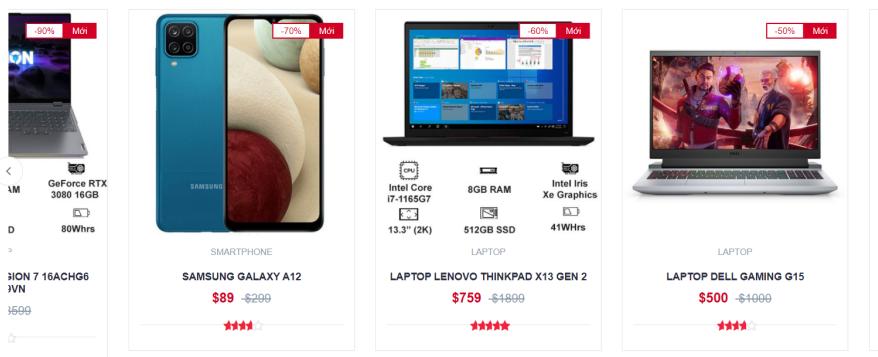
LAPTOP SMARTPHONE



Hình 6: Màn hình trang chủ hiển thị quảng cáo

CHƯƠNG TRÌNH KHUYẾN MÃI

LAPTOP SMARTPHONE



Hình 7: Màn hình trang chủ hiển thị chương trình khuyến mãi



The screenshot shows three separate promotional sections, each titled "GIÁ SỐC" (Big Sale). Each section displays a grid of discounted items:

- Section 1:** Shows a laptop (Lenovo Legion 7 1), a smartphone (Realme 7 Pro), and a laptop (Lenovo Yoga 6 13ALC6).
- Section 2:** Shows a smartphone (Samsung Galaxy A12) and a smartphone (iPhone 12 Mini).
- Section 3:** Shows a smartphone (Realme 7 Pro) and a laptop (Lenovo Yoga 6 13ALC6).

Below these sections is a newsletter sign-up form with fields for email and social media links.

Hình 8: Màn hình trang chủ hiển thị giá sốc

4.3.4 Màn hình liên hệ

The screenshot shows the contact page of the BK Computer website. It features a header with the logo, search bar, and user account information. Below the header is a map of the KTX A area in HCMC, showing the location of the store and nearby landmarks. To the right of the map is a sidebar with contact details:

- Cửa hàng BK Computer**
- Địa chỉ: KTX khu A, Đại học Quốc gia TP.HCM
- Số điện thoại: 0919523753
- Email: vu.le08@hcmut.edu.vn
- Giờ làm việc: 8:00 - 17:30, T2-T7

Hình 9: Màn hình liên hệ



4.3.5 Màn hình tìm kiếm sản phẩm

The screenshot shows the BK Computer website's search results for the term "apple". The search bar at the top contains "apple". Below it, a dropdown menu lists several Apple products: "Apple iMac 27 5K 2020 i5", "Apple MacBook Pro 13 Touch Bar M1", "Apple Macbook Pro 16 Touch Bar I7", and "Apple Macbook Pro 16 Touch Bar I7 2.6 16GB 512GB". The main content area displays three laptop products: an iMac 2021 (M1 8GPU 16GB 512GB) for \$2299, an Apple MacBook Pro 16 Touch Bar (I7 2.6 16GB 512GB) for \$2069, and another Apple MacBook Pro 16 Touch Bar (I7) for \$1872. The interface includes filters for category (Laptop, Smartphone), price range (50 - 5000), brand (ASUS, DELL, APPLE), and sorting by price from high to low.

Hình 10: Màn hình tìm kiếm sản phẩm

4.3.6 Màn hình chính sách bảo mật

The screenshot shows the BK Computer website's Privacy Policy page. The URL in the address bar is "https://www.bkcomputer.vn/chinh-sach-bao-mat". The page title is "Chính sách bảo mật". The content is divided into sections: "Điều khoản và Bảo mật", "Bảo vệ dữ liệu cá nhân và giao dịch", "Thu thập thông tin cá nhân", and "Chính sách cookie". It includes detailed text about data protection, privacy rights, and cookie usage, along with legal disclaimers and contact information.

Hình 11: Màn hình chính sách bảo mật



4. Quyền lợi khách hàng

Quý khách có quyền yêu cầu truy cập vào dữ liệu cá nhân của mình, có quyền yêu cầu chúng tôi sửa lại những sai sót trong dữ liệu của bạn mà không mất phí. Bất cứ lúc nào bạn cũng có quyền yêu cầu chúng tôi ngưng sử dụng dữ liệu cá nhân của bạn cho mục đích tiếp thị.

Đăng ký nhận Tin tức mới

f i o

THÔNG TIN LIÊN HỆ	DANH MỤC NỔI BẬT	THÔNG TIN CỦA HÀNG	DỊCH VỤ
Chào mừng bạn đến với ngôi nhà BK Computer! Tại đây, mỗi một dòng chữ, mỗi chi tiết và hình ảnh đều là những bằng chứng mang dấu ấn, và đang không ngừng phát triển lớn mạnh.	Ưu đãi lớn Laptops Smartphones	Giới thiệu Liên hệ Chính sách bảo mật	Tài khoản của tôi
📍 KTX khu A, Đại học Quốc gia TP.HCM 📞 0919523753 ✉ vu.le08@hcmut.edu.vn			

Hình 12: Màn hình chính sách bảo mật

4.3.7 Màn hình giới thiệu

Hình 13: Màn hình giới thiệu





SẢN PHẨM TỐT NHẤT

Cùng với đó cung cấp thời gian bảo hành máy dài, dịch vụ hậu mãi tốt cho khách hàng yên tâm sử dụng sản phẩm. Mức giá bán sản phẩm máy tính laptop cũ, linh kiện máy tính cũng ở mức hợp lý, phái chặng, rất tương xứng chất lượng.

 **Miễn phí giao hàng**
Tại đây, mỗi một dòng chữ, mỗi chi tiết và hình ảnh đều là những bảng chứng mang dấu ấn lịch sử Converse 100 năm, và đang không ngừng phát triển lớn mạnh

 **Đổi trả trong vòng 7 ngày**
Tại đây, mỗi một dòng chữ, mỗi chi tiết và hình ảnh đều là những bảng chứng mang dấu ấn lịch sử Converse 100 năm, và đang không ngừng phát triển lớn mạnh

 **Sản phẩm mới 100%**
Tại đây, mỗi một dòng chữ, mỗi chi tiết và hình ảnh đều là những bảng chứng mang dấu ấn lịch sử Converse 100 năm, và đang không ngừng phát triển lớn mạnh

 **Chăm sóc khách hàng**
Tại đây, mỗi một dòng chữ, mỗi chi tiết và hình ảnh đều là những bảng chứng mang dấu ấn lịch sử Converse 100 năm, và đang không ngừng phát triển lớn mạnh

 **Hàng chính hãng**
Tại đây, mỗi một dòng chữ, mỗi chi tiết và hình ảnh đều là những bảng chứng mang dấu ấn lịch sử Converse 100 năm, và đang không ngừng phát triển lớn mạnh

 **Thanh toán đa dạng**
Tại đây, mỗi một dòng chữ, mỗi chi tiết và hình ảnh đều là những bảng chứng mang dấu ấn lịch sử Converse 100 năm, và đang không ngừng phát triển lớn mạnh

Hình 14: Màn hình giới thiệu sản phẩm

là những bảng chứng mang dấu ấn lịch sử Converse 100 năm, và đang không ngừng phát triển lớn mạnh

là những bảng chứng mang dấu ấn lịch sử Converse 100 năm, và đang không ngừng phát triển lớn mạnh

Thành viên nhóm



Lê Tuấn Vũ
QUẢN LÝ

[f](#) [in](#) [o](#)



Nguyễn Thế Viễn
GIAM ĐỐC

[f](#) [in](#) [o](#)



Đào Thanh Tú
QUẢN LÝ

[f](#) [in](#) [o](#)

Hình 15: Màn hình giới thiệu thành viên nhóm



4.3.8 Màn hình trang hiển thị sản phẩm

DANH MỤC

SẮP XẾP THEO: Giá từ cao đến thấp HIỂN THỊ: 9

LAPTOP

SMARTPHONE

GIÁ

THƯƠNG HIỆU

ASUS

DELL

APPLE

HP

HUAWEI

LENOVO

OPPO

REALME

SAMSUNG

LAPTOP DELL LATITUDE 3520 70251590
\$1020 - \$1200
★★★★★

LAPTOP DELL ALIENWARE M15 R6 P109F001ABL
\$1012 - \$1100
★★★★★

LAPTOP DELL VOSTRO 3500 P112F002ABL
\$935 - \$1100
★★★★★

LAPTOP DELL GAMING G15
\$500 - \$1000
★★★★★

LAPTOP DELL INSPIRON I3501-5075BLK
\$899 - \$999
★★★★★

SMARTPHONE

Hình 16: Màn hình hiển thị sản phẩm giá từ cao đến thấp

DANH MỤC

SẮP XẾP THEO: Giá từ thấp đến cao HIỂN THỊ: 18

LAPTOP

SMARTPHONE

GIÁ

THƯƠNG HIỆU

ASUS

DELL

APPLE

HP

HUAWEI

LENOVO

OPPO

REALME

SAMSUNG

LAPTOP DELL GAMING G15
\$500 - \$1000
★★★★★

LAPTOP DELL INSPIRON I3501-5075BLK
\$899 - \$999
★★★★★

LAPTOP DELL VOSTRO 3500 P90F006CBL
\$900 - \$1000
★★★★★

LAPTOP DELL LATITUDE 3520 70251590
\$1020 - \$1200
★★★★★

LAPTOP DELL ALIENWARE M15 R6 P109F001ABL
\$1012 - \$1100
★★★★★

SMARTPHONE

Hình 17: Màn hình hiển thị sản phẩm giá từ thấp đến cao



DANH MỤC

SẮP XẾP THEO: Khuyến Mãi HIỂN THỊ: 18

LAPTOP
 SMARTPHONE

GIÁ

THƯƠNG HIỆU

ASUS
 DELL
 APPLE
 HP
 HUAWEI
 LENOVO
 OPPO
 REALME
 SAMSUNG

Tên Sản Phẩm	Giá	Mã Giảm Giá
LAPTOP DELL GAMING G15	\$500 - \$1000	-50% Mới
LAPTOP DELL LATITUDE 3520 70251590	\$1020 - \$1200	-15% Mới
LAPTOP DELL VOSTRO 3500 P112F002ABL	\$935 - \$4400	-15% Mới
(Laptop 1)		-10% Mới
(Laptop 2)		-10% Mới
(Laptop 3)		-8% Mới

Hình 18: Màn hình hiển thị sản phẩm theo khuyến mãi

DANH MỤC

SẮP XẾP THEO: Năm phát hành HIỂN THỊ: 18

LAPTOP
 SMARTPHONE

GIÁ

THƯƠNG HIỆU

ASUS
 DELL
 APPLE
 HP
 HUAWEI
 LENOVO
 OPPO
 REALME
 SAMSUNG

Tên Sản Phẩm	Giá	Mã Giảm Giá
OPPO A95	\$367 - \$399	-8% Mới
OPPO A74	\$321 - \$349	-10% Mới
OPPO RENO6 5G	\$551 - \$699	-8% Mới
(Smartphone 1)		-8% Mới
(Smartphone 2)		-8% Mới
(Smartphone 3)		-50% Mới

Hình 19: Màn hình hiển thị sản phẩm theo năm phát hành



4.3.9 Màn hình hiển thị chi tiết sản phẩm

Hình 20: Màn hình hiển thị chi tiết sản phẩm

4.3.10 Màn hình trang hiển thị thông số kỹ thuật sản phẩm

Hãng sản xuất	Dell
Năm sản xuất	2021
CPU	AMD Ryzen 5 - 5600H
RAM	8 GB
Ổ cứng	256 GB SSD NVMe PCIe (Có thể tháo ra, lắp thanh khác tối đa 2TB (2280) / 1TB (2230))Không hỗ trợ khe cắm HDD
Card đồ họa	RTX 3050 4GB
Màn hình	15.6"Full HD (1920 x 1080)120Hz
Hệ điều hành	Windows 11 Home SL + Office Home & Student 2021 vĩnh viễn
Pin	3-cell Li-ion, 56 Wh
Camera trước	8MG
Độ nặng	1.5

Đăng ký nhận Tin tức mới

Nhập email...

Hình 21: Màn hình hiển thị thông số kỹ thuật



4.3.11 Màn hình trang hiển thị đánh giá, bình luận

The screenshot shows a product review section. At the top, there is a small image of a laptop. Below it, a navigation bar includes 'Mô tả', 'Thông số kỹ thuật', and 'Bình luận' (which is highlighted in red). A rating of 4.54 with five stars is displayed, along with a slider for each star from 1 to 5. There are three reviews listed:

- tuanvu (Nov 30, 2021 10:46 AM) - ok
- tuanvu (Nov 30, 2021 9:32 AM) - ok
- ntvien (Nov 30, 2021 9:23 AM) - Em mới mua sản phẩm này ở shop, giá cả hợp lý, giá tiền vừa phải

A large text area labeled 'Bình luận của bạn' is provided for users to enter their own comments. Below it, a 'Đánh giá của bạn:' slider shows five stars, and a red 'BÌNH LUẬN' button is visible. A navigation bar at the bottom shows pages 1 through 5.

Below this section, there is a 'Đăng ký nhận Tin tức mới' (Subscribe to new news) form with fields for email and social media links (Facebook, Email, Google+).

Hình 22: Màn hình hiển thị đánh giá, bình luận

4.3.12 Màn hình thông tin đặt hàng

The screenshot shows a checkout page. At the top, there is a navigation bar with links: Trang chủ, Cửa hàng, Giới thiệu, Liên hệ, Chính sách bảo mật.

The main form is divided into two sections:

- ĐẠI CHỈ THANH TOÁN**: Contains fields for Name (*), Last name (*), Email (*), Phone number (*), Address (*), and Note.
- ĐƠN HÀNG CỦA BẠN**: A summary table showing items, prices, and total.

Sản phẩm	Giá tiền
2x Laptop Dell Gaming G15	\$1000.00
4x iPhone 13 Pro Max	\$5036.40
Shipping	Miễn phí
Tổng tiền	\$6036.40

Below the table, there is a list of payment methods with radio buttons:

- Chuyển khoản trực tiếp
- Thanh toán tiền mặt khi nhận hàng
- Thanh toán bằng ví ZaloPay
- Thanh toán bằng ví MoMo
- Thanh toán bằng thẻ quốc tế Visa, Master, JCB

A red 'ĐẶT HÀNG' button is located at the bottom right of the summary table.

Hình 23: Màn hình hiển thị thông tin đặt hàng



4.3.13 Màn hình thay đổi thông tin cá nhân

Thông tin của tôi

Tên đăng nhập

Email

Chúng tôi sẽ không chia sẻ email của bạn cho bất kỳ ai.

Họ Tên

Số điện thoại

Địa chỉ

Mật khẩu hiện tại

Hình 24: Màn hình hiển thị thay đổi thông tin cá nhân

4.3.14 Màn hình thay đổi mật khẩu

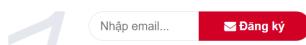
dak nong

Mật khẩu hiện tại

Mật khẩu mới

Mật khẩu mới (xác nhận)

Đăng ký nhận Tin tức mới



Hình 25: Màn hình hiển thị thay đổi mật khẩu



4.3.15 Màn hình admin quản lý đơn hàng

ID	ID khách hàng	Tên	Họ tên lót	Thời gian đặt hàng	Địa chỉ	Số điện thoại	Email
34	8	Vũ	Lê	Nov 30, 2021 10:46 AM	dak nong	0919523753	vu@gmail.cor
33	8	Vũ	Lê	Nov 30, 2021 9:32 AM	dak nong	0919523753	vu@gmail.cor
32	8	Vũ	Lê	Nov 30, 2021 9:21 AM	dak nong	0919523753	vu@gmail.cor
24	8	Vũ	Lê Tuấn	Nov 29, 2021 9:54 PM	dak nong	0919523753	vu@gmail.cor
23	8	Vũ	Lê Tuấn	Nov 29, 2021 9:53 PM	dak nong	0919523753	vu@gmail.cor
22	15	Viễn	Nguyễn Thủ Viễn	Nov 29, 2021 5:46 PM	99 Phú Mỹ, quận Bình Th...	0367190549	thevien898@q...
21	15	Viễn	Nguyễn Thủ Viễn	Nov 29, 2021 5:42 PM	99 Phú Mỹ, quận Bình Th...	0367190549	thevien898@q...
20	8	Vu	le tuan	Nov 29, 2021 4:57 PM	dak nong	0919523753	vu@gmail.cor
19	8	Vu	le tuan	Nov 29, 2021 4:16 PM	dak nong	0919523753	vu@gmail.cor
18	8	Vu	le tuan	Nov 29, 2021 1:23 PM	dak nong	0919523753	vu@gmail.cor

Hình 26: Màn hình admin quản lý đơn hàng

4.3.16 Màn hình admin quản lý tài khoản người dùng

ID	Tên đăng nhập	Tên	Họ tên lót	Email	Địa chỉ	Số điện thoại	Vai trò
8	tuanvu	Vũ	Lê	vu@gmail.com	dak nong	0919523753	admin
10	tudao	Tu	Đao Thanh	tu@gmail.com	Bien Hoa	0919523753	admin
11	thevien	Viên	Nguyễn Thủ	thevien@gmail.c...	Gia Lai	09324545645	admin
12	tu123		Dao	tu@gmail.com	bien hoa		customer
13	tudaobku	Tú	Đao	tu@gmail.com	Bien Hoa	0919523753	customer
15	ntvien	viễn	Nguyễn Thủ	thevien898@gm...	99 Phú Mỹ, quận Bình T...	0367190549	customer
18	admin		vu	vu@gmail.com			admin
19	tuanvu2323			dsa@gmail.com			customer

Hình 27: Màn hình admin quản lý tài khoản người dùng



4.3.17 Màn hình admin tạo tài khoản mới

The screenshot shows a modal dialog titled "Tạo tài khoản mới" (Create New Account) overlaid on a list of users. The modal contains fields for "Tên đăng nhập" (Login Name) set to "admin", "Mật khẩu" (Password) set to "*****", and "Email" set to "thevien898@gmail.com". Under "Vai trò" (Role), the "Quản trị viên" (Administrator) radio button is selected. At the bottom are two buttons: "ĐÓNG" (Close) and "LƯU" (Save). The background list shows 8 users with IDs 8 through 15, names like tuanvu, tudao, thevien, tu123, tudaobku, ntvlien, admin, and tuanvu23, along with their roles (admin or customer) and contact details.

Hình 28: Màn hình admin tạo tài khoản mới

4.3.18 Màn hình admin quản lý sản phẩm

The screenshot shows a list of products with columns for ID, Product Name, Manufacturer, Price, Discount (%), and Release Year. The products listed are:

ID sản phẩm	Tên sản phẩm	Tên thương hiệu	Giá tiền	Giảm giá(%)	Năm phát hành
48	Laptop Lenovo Legion 7 16ACHG6 82N6003...	Lenovo	3599	90	2021
71	iMac 24 2021 M1 8GPU 16GB 512GB	Apple	2499	8	2021
36	Apple Macbook Pro 16 Touch Bar i7	Apple	2400	22	2019
72	Apple Macbook Pro 16 Touch Bar i7 2.6 16G...	Apple	2299	10	2019
19	Apple iMac 27 K 2020 i5	Apple	2005	7	2020
18	Apple MacBook Pro 13 Touch Bar M1	Apple	2000	10	2020
49	Laptop Lenovo Thinkpad X13 GEN 2	Lenovo	1899	60	2021
66	iPhone 13 Pro Max	Apple	1399	10	2021
41	Laptop ASUS TUF Gaming FA506QR-AZ003T	Asus	1299	8	2021
15	Laptop Dell Latitude 3520 70251590	Dell	1200	15	2021

At the bottom are buttons for "THÊM THƯƠNG HIỆU" (Add Brand) and "THÊM SẢN PHẨM" (Add Product). The page footer indicates "1-10 of 42".

Hình 29: Màn hình admin quản lý sản phẩm



4.3.19 Màn hình admin quản lý sản phẩm thêm thương hiệu

The screenshot shows a list of products on the left and a modal window on the right for adding a brand. The modal has fields for 'Tên thương hiệu*' (Brand name*) and 'Logo thương hiệu' (Brand logo), both of which are currently empty. There are 'ĐÓNG' (Close) and 'LƯU' (Save) buttons at the bottom of the modal.

Hình 30: Màn hình admin quản lý sản phẩm thêm thương hiệu

4.3.20 Màn hình admin quản lý thay đổi sản phẩm

The screenshot shows a detailed edit form for a product. The product ID is 48, and the name is 'Laptop Lenovo Legion 7 16ACHC'. The form includes fields for price (3599), discount (90%), product type (laptop), year (2021), CPU (AMD Ryzen 9 5900HX 3.3GHz), RAM (32GB), screen resolution (2560 x 1600 pixel (2K)), operating system (Windows 10 Home SL), SIM card (Mô tả SIM), battery (4 Cell 80 Whr), and a detailed description (Laptop Lenovo Legion 7). There are also fields for back camera (Camera sau), front camera (Camera trước), and logos (Hình ảnh chính, Hình ảnh phụ). Buttons for 'TẠO SẢN PHẨM MỚI' (Create New Product) and 'LƯU' (Save) are at the bottom.

Hình 31: Màn hình admin quản lý thay đổi sản phẩm



4.3.21 Màn hình admin quản lý đánh giá, bình luận

The screenshot shows a web-based administrative interface for managing reviews and comments. On the left, there is a sidebar with four menu items: Đơn hàng (Orders), Người dùng (Users), Sản Phẩm (Products), and Đánh giá (Reviews). The 'Đánh giá' item is currently selected and highlighted in grey. The main content area displays a table with 10 columns: ID bình luận, ID khách hàng, Tên đăng nhập, ID sản phẩm, Tên sản phẩm, Thời gian bình luận, Xếp hạng, and Nội dung bình luận. The table contains 10 rows of data, each representing a review or comment. The first three rows have checkboxes checked, indicating they are selected. The last row shows a message about a phone being damaged. At the bottom of the table, it says '3 rows selected'. Below the table, there are navigation arrows for pagination, showing '1-10 of 34'. A blue button labeled 'XOÁ' (Delete) is located at the bottom right of the table area.

ID bình luận	ID khách hàng	Tên đăng nhập	ID sản phẩm	Tên sản phẩm	Thời gian bình luận	Xếp hạng	Nội dung bình luận
54	8	tuanvu	12	Laptop Dell Gaming ...	Jan 20, 1970 6:04 AM	3	ok
50	8	tuanvu	15	Laptop Dell Latitude ...	Jan 20, 1970 6:04 AM	5	ok
49	15	ntvien	19	Apple iMac 27 5K 20...	Jan 20, 1970 6:04 AM	4	Sản phẩm bên shop ch
48	8	tuanvu	12	Laptop Dell Gaming ...	Jan 20, 1970 6:03 AM	5	ok
47	15	ntvien	12	Laptop Dell Gaming ...	Jan 20, 1970 6:03 AM	5	Em mới mua sản phẩm
46	13	tudaobku	14	Laptop Dell Vostro 3...	Jan 20, 1970 6:03 AM	3	Đẹp lắm
45	13	tudaobku	14	Laptop Dell Vostro 3...	Jan 20, 1970 6:03 AM	2	Ok lắm
44	13	tudaobku	14	Laptop Dell Vostro 3...	Jan 20, 1970 6:03 AM	5	Tuyệt
43	13	tudaobku	12	Laptop Dell Gaming ...	Jan 20, 1970 6:03 AM	4	Màu đen
42	17	vu	61	Samsung Galaxy A5...	Jan 20, 1970 6:03 AM	5	điện thoại sài rất ok

Hình 32: Màn hình admin quản lý đánh giá, bình luận



5 Cách thức cài đặt ứng dụng

5.1 Yêu cầu hệ thống

- Sử dụng hệ điều hành Window 10, Linux, MacOS.
- Có cài đặt PHP phiên bản mới nhất.

5.2 Cách khởi động website

1. Khởi động chạy **backend**:

- Vào thư mục **backend**.
- Tiếp đến vào thư mục **public**.
- Thực hiện câu lệnh: `php -S localhost:8082 ./index.php`

2. Khởi động chạy **frontend**:

- Vào thư mục **frontend**.
- Đầu tiên, chạy lệnh **yarn** để tải các thư viện, package cần thiết.
- Tiếp đến, chạy lệnh **yarn start**.

3. Truy cập theo đường dẫn: <https://localhost:3000>



6 Đánh giá

6.1 Đánh giá kết quả đạt được

1. Thiết kế, hiện thực được giao diện cho trang web, có thể tương thích với nhiều loại màn hình khác nhau như laptop, điện thoại, máy tính bảng.
2. Thực hiện được các chức năng cho các đối tượng khác nhau:
 - **Khách hàng:** xem thông tin các sản phẩm trên trang web, cho phép đăng ký hoặc đăng nhập, tìm kiếm sản phẩm, xem chi tiết sản phẩm, trang liên hệ, trang chính sách bảo mật.
 - **Thành viên (sau khi đã đăng nhập):** ngoài có các chức năng như khách hàng thì còn có thể đặt hàng, thay đổi thông tin cá nhân, thay đổi mật khẩu, đăng xuất, viết bình luận đánh giá,...
 - **Admin:** admin có thể quản lý khách hàng, nhân viên, các sản phẩm, các đơn hàng, bình luận của khách hàng và các phản hồi của khách hàng về sản phẩm cũng như dịch vụ.

6.2 Hướng phát triển trong tương lai

- Cải thiện giao diện để người dùng dễ dàng thao tác và cung cấp thêm nhiều tác vụ.
- Thêm một số hình thức đăng ký tài khoản bằng các mạng xã hội đã có như Facebook, Instagram, Gmail,...
- Tái cấu trúc một số chức năng cũng như toàn bộ hệ thống để dễ cho việc quản lý, nâng cấp về sau.
- Thêm tính năng thanh toán trực tuyến bằng thẻ ngân hàng/atm.
- Tích hợp các chương trình bảo mật lên website để nâng cao tính an toàn cho người dùng.

6.3 Đánh giá mức độ thực hiện của các thành viên

STT	MSSV	Họ và tên	Nhiệm vụ
1	1814764	Nguyễn Thế Viễn	Hiện thực template phía khách hàng, hiện thực chức năng trang chủ, trang liên hệ và giới thiệu, chính sách bảo mật, trang đăng nhập, đăng ký, test lỗi và viết báo cáo.
2	1814656	Dào Thanh Tú	Hiện thực tìm kiếm sản phẩm, trang thông tin người dùng, trang chi tiết sản phẩm, viết bình luận, đánh giá, xử lý backend, test lỗi và viết báo cáo.
3	1814812	Lê Tuấn Vũ	Hiện thực template phía admin, hiện thực chức năng trang admin quản lý khách hàng, đơn hàng, đánh giá, sản phẩm, xử lý backend, test lỗi và viết báo cáo.



Tài liệu

- [1] Reactjs [online], from: <https://reactjs.org/docs/getting-started.html>, viewed 25/10/2021.
- [2] Bootstrap [online], from: <https://getbootstrap.com/docs/5.1/getting-started/introduction/>, viewed 25/10/2021.
- [3] Font Awesome [online], from: <https://fontawesome.com/v5.15/icons>, viewed 25/10/2021.
- [4] PHP [online], from: <https://www.php.net/docs.php>, viewed 25/10/2021.
- [5] Material UI [online], from: <https://mui.com/getting-started/usage/>, viewed 25/10/2021.
- [6] Slick [online], from: <https://kenwheeler.github.io/slick/>, viewed 25/10/2021.
- [7] Mysql [online], from: <https://dev.mysql.com/doc/>, viewed 25/10/2021.