BAN CƠ YẾU CHÍNH PHỦ

**HỌC VIỆN KỸ THUẬT MẬT MÃ**

ĐỒ ÁN TỐT NGHIỆP

# XÂY DỰNG WEBSITE THƯƠNG MẠI ĐIỆN TỬ AN TOÀN

Ngành: An toàn thông tin

Mã số: 7.48.02.02

Thành phố Hồ Chí Minh, 2023

BAN CƠ YẾU CHÍNH PHỦ

**HỌC VIỆN KỸ THUẬT MẬT MÃ**

ĐỒ ÁN TỐT NGHIỆP

# XÂY DỰNG WEBSITE THƯƠNG MẠI ĐIỆN TỬ AN TOÀN

Ngành: An toàn thông tin

Mã số: 7.48.02.02


*Sinh viên thực hiện*:

**Ngô Quang Sang**

Lớp: AT15H

*Người hướng dẫn*:

**ThS. Vũ Thị Vân**

Khoa An toàn thông tin - Học viện Kỹ thuật mật mã


Thành phố Hồ Chí Minh, 2023

# LỜI CẢM ƠN

# LỜI CAM ĐOAN

# MỤC LỤC

**LỜI CẢM ƠN** ..... i
**LỜI CAM ĐOAN** ..... ii
**MỤC LỤC** ..... iii
**DANH MỤC CÁC KÝ HIỆU, CHỮ VIẾT TẮT** ..... vi
**DANH MỤC BẢNG** ..... vii
**DANH MỤC HÌNH VẼ, ĐỒ THỊ** ..... viii
**MỞ ĐẦU** ..... 1
**CHƯƠNG 1. KHẢO SÁT VÀ XÁC ĐỊNH YÊU CẦU SẢN PHẨM** ..... 2
**1.1. Khái niệm và tính năng của website thương mại điện tử (TMĐT)** ..... 2
**1.2. Các yếu tố quan trọng trong thiết kế website TMĐT** ..... 2
*1.2.1. Trải nghiệm người dùng (User Experience - UX)* ..... 2
*1.2.2. Thiết kế Responsive* ..... 2
*1.2.3. Tối ưu hóa tốc độ load trang* ..... 2
**1.3. Giải pháp quản lý dữ liệu khách hàng và đơn hàng hiệu quả** ..... 2
*1.3.1. Khái niệm và tính chất của dữ liệu khách hàng và đơn hàng* ..... 2
*1.3.2. Các giải pháp quản lý dữ liệu hiệu quả* ..... 2
**1.4. Các lỗi bảo mật phổ biến trong website TMĐT và cách khắc phục** ..... 3
*1.4.1. SQL Injection* ..... 3
*1.4.2. Cross-Site Scripting (XSS)* ..... 4
*1.4.3. Cross-Site Request Forgery (CSRF)* ..... 5
*1.4.4. Broken Authentication* ..... 5
*1.4.5. Injection Flaw* ..... 6
**1.5. Giải pháp xác thực an toàn bảo mật cho dữ liệu và thanh toán** ..... 6
*1.5.1. SSL - Secure Socket Layer* ..... 6
*1.5.2. Tokenization* ..... 6
*1.5.3. 3D Secure* ..... 6
*1.5.4. PCI DSS Compliance* ..... 6
*1.5.5. OAuth* ..... 6
*1.5.6. Secure Payment Protocols* ..... 6
**1.6. Kết chương** ..... 6
**CHƯƠNG 2. PHÂN TÍCH VÀ THIẾT KẾ WEBSITE TMĐT** ..... 7
**2.1. Mô tả bài toán** ..... 7
**2.2. Phân tích nghiệp vụ và yêu cầu chức năng** ..... 7
*2.2.1. Chức năng đăng nhập và đăng ký tài khoản* ..... 7
*2.2.2. Chức năng tìm kiếm sản phẩm* ..... 8
*2.2.3. Chức năng giỏ hàng và thanh toán* ..... 8

*2.2.4. Chức năng quản lý thông tin tài khoản và đơn hàng* ..... 8
**2.3. Thiết kế giao diện và trải nghiệm người dùng** ..... 9
*2.3.1. Thiết kế giao diện* ..... 9
*2.3.2. Trải nghiệm người dùng* ..... 9
**2.4. Thiết kế cơ sở dữ liệu** ..... 9
*2.4.1. Lựa chọn hệ quản trị cơ sở dữ liệu* ..... 9
*2.4.2. Thiết kế mô hình dữ liệu* ..... 9
*2.4.3. Thiết kế quan hệ giữa các bảng dữ liệu* ..... 9
*2.4.4. Thiết kế các truy vấn và thủ tục lưu trữ* ..... 9
*2.4.5. Phân tích và tối ưu hóa hiệu suất cơ sở dữ liệu* ..... 9
*2.4.6. Đảm bảo tính nhất quán và an toàn cho cơ sở dữ liệu* ..... 9
**2.5. Phân tích thiết kế kiến trúc hệ thống** ..... 9
*2.5.1. Xác định các thành phần của hệ thống* ..... 9
*2.5.2. Thiết kế và xây dựng kiến trúc hệ thống* ..... 9
*2.5.3. Đánh giá hiệu năng và khả năng mở rộng của hệ thống* ..... 10
*2.5.4. Áp dụng các tiêu chuẩn trong thiết kế kiến trúc hệ thống* ..... 10
**2.6. Đảm bảo an toàn và bảo mật cho website** ..... 10
*2.6.1. Sử dụng HTTPS để bảo mật kết nối* ..... 10
*2.6.2. Xác thực người dùng và quản lý phiên làm việc* ..... 10
*2.6.3. Kiểm tra dữ liệu đầu vào và đầu ra* ..... 10
*2.6.4. Áp dụng các giải pháp bảo mật như CAPTCHA, ReCaptcha* ..... 10
*2.6.5. Theo dõi và giám sát hệ thống thường xuyên* ..... 10
**2.7. Quản lý và bảo vệ thông tin khách hàng trên website TMĐT** ..... 10
*2.7.1. Quản lý thông tin cá nhân và dữ liệu khách hàng* ..... 10
*2.7.2. Bảo vệ thông tin giao dịch trên website TMĐT* ..... 10
*2.7.3. Các qui định pháp lý liên quan* ..... 10
**2.8. Kết chương** ..... 10
**CHƯƠNG 3. XÂY DỰNG SẢN PHẨM** ..... 11
**3.1. Môi trường phát triển và công nghệ sử dụng** ..... 11
**3.2. Các bước triển khai** ..... 11
*3.2.1. Chuẩn bị môi trường phát triển* ..... 11
*3.2.2. Thiết kế giao diện và trải nghiệm người dùng* ..... 12
*3.2.3. Lập trình các chức năng và tính năng* ..... 12
*3.2.4. Đảm bảo an toàn và bảo mật cho website* ..... 12
*3.2.5. Triển khai website TMĐT* ..... 12
**3.3. Kiểm thử và nâng cao chất lượng sản phẩm** ..... 12
*3.3.1. Kiểm thử chức năng* ..... 12
*3.3.2. Kiểm thử hiệu suất và tải trang* ..... 12
*3.3.3. Kiểm thử bảo mật* ..... 12
*3.3.4. Nâng cao chất lượng sản phẩm* ..... 12

**3.4. Quản lý và vận hành website** ..... 12
*3.4.1. Quản lý nội dung website* ..... 12
*3.4.2. Quản lý danh mục sản phẩm và kho hàng* ..... 12
*3.4.3. Quản lý đơn hàng và thanh toán* ..... 12
*3.4.4. Quản lý khách hàng và dịch vụ hỗ trợ* ..... 12
**3.5. Kết chương** ..... 12
**CHƯƠNG 4. PHỤ LỤC** ..... 13
**4.1. Ưu nhược điểm của các website TMĐT** ..... 13
**CHƯƠNG 5. TÀI LIỆU THAM KHẢO** ..... 14

# DANH MỤC CÁC KÝ HIỆU, CHỮ VIẾT TẮT

# DANH MỤC BẢNG

# DANH MỤC HÌNH VẼ, ĐỒ THỊ

# MỞ ĐẦU

Số lượng người dùng TMĐT tăng nhanh: Gần đây, sự phát triển công nghệ mở ra nhiều cơ hội kinh doanh mới, giúp thị trường TMĐT phát triển và thu hút nhiều người dùng hơn.

Vấn đề an toàn và bảo mật trong TMĐT: Khi giao dịch trực tuyến, người dùng thường cung cấp thông tin cá nhân và tài khoản ngân hàng. Nếu không có biện pháp bảo mật, dữ liệu này có thể bị đánh cắp và lợi dụng để gây hại.

Mục tiêu chính của đề tài này là tạo ra sản phẩm nhằm tăng cường an toàn và bảo mật trong TMĐT: Triển khai giải pháp xá c thực an toàn bảo mật cho dữ liệu và thanh toán giúp tăng cường an toàn và bảo mật cho giao dịch TMĐT, giúp người dùng yên tâm hơn khi giao dịch trực tuyến.

Nâng cao uy tín và chất lượng của website TMĐT: Khi website TMĐT triển khai các giải pháp bảo mật an toàn và đáp ứng các tiêu chuẩn an toàn quốc tế, đó là điểm cộng để nâng cao uy tín và chất lượng của website, thu hút người dùng tin tưởng và sử dụng.

Đóng góp tích cực cho sự phát triển của TMĐT: TMĐT đang trở thành lĩnh vực kinh doanh tiềm năng, đóng góp tích cực cho sự phát triển của nền kinh tế và xã hội. Triển khai giải pháp bảo mật an toàn cho TMĐT giúp tạo điều kiện thuận lợi cho sự phát triển của lĩnh vực này, giúp doanh nghiệp TMĐT tăng cường sự tin tưởng của khách hàng và nâng cao hiệu quả kinh doanh.

Đáp ứng các tiêu chuẩn và quy định của pháp luật: Hiện nay, các quy định vềbảo mật thông tin và thanh toán trực tuyến đang được nhiều quốc gia và khu vực áp dụng. Triển khai giải pháp bảo mật an toàn cho TMĐT giúp đáp ứng các tiêu chuẩn và quy định này, giúp website TMĐT tránh được các rủi ro về pháp lý.

Vì vậy, đề tài này có tính cấp thiết và ý nghĩa thực tiễn cao, giúp tăng cường an toàn và bảo mật cho giao dịch TMĐT, đóng góp tích cực cho sự phát triển của lĩnh vực TMĐT và đáp ứng các tiêu chuẩn và quy định của pháp luật.

# CHƯƠNG 1. KHẢO SÁT VÀ XÁC ĐỊNH YÊU CẦU SẢN PHẨM

## 1.1. Khái niệm và tính năng của website thương mại điện tử (TMĐT)

## 1.2. Các yếu tố quan trọng trong thiết kế website TMĐT

### *1.2.1. Trải nghiệm người dùng (User Experience - UX)*

### *1.2.2. Thiết kế Responsive*

### *1.2.3. Tối ưu hóa tốc độ load trang*

## 1.3. Giải pháp quản lý dữ liệu khách hàng và đơn hàng hiệu quả

### *1.3.1. Khái niệm và tính chất của dữ liệu khách hàng và đơn hàng*

### *1.3.2. Các giải pháp quản lý dữ liệu hiệu quả*

#### *1.3.2.1. CRM - Customer Relationship Management*

CRM (Customer Relationship Management) là một phương pháp quản lý, tương tác và liên kết với khách hàng của doanh nghiệp. Trong website TMĐT, CRM được sử dụng để quản lý thông tin khách hàng, ghi nhận các hoạt động liên quan đến khách hàng và xây dựng quan hệ tốt hơn với khách hàng.

Trong website TMĐT, CRM có thể bao gồm các tính năng sau:

- Quản lý thông tin khách hàng: Hệ thống CRM cho phép lưu trữ và quản lý thông tin chi tiết về khách hàng, bao gồm tên, địa chỉ, số điện thoại, email, lịch sử mua hàng, câu hỏi và yêu cầu của khách hàng.
- Quản lý hoạt động liên quan đến khách hàng: Hệ thống CRM cho phép ghi nhận các hoạt động liên quan đến khách hàng như cuộc gọi điện thoại, email và tin nhắn, lịch hẹn, giải đáp thắc mắc của khách hàng,…
- Quản lý bán hàng: Hệ thống CRM cũng hỗ trợ quản lý quá trình bán hàng từ việc tìm kiếm khách hàng tiềm năng đến việc tạo đơn hàng và theo dõi thanh toán.
- Xây dựng quan hệ tốt hơn với khách hàng: Hệ thống CRM giúp xác định được nhu cầu và yêu cầu của khách hàng, từ đó đưa ra các chiến lược phù hợp để nâng cao chất lượng dịch vụ, tạo sự tin tưởng và tăng cường sự hài lòng của khách hàng.

#### *1.3.2.2. Quản lý đơn hàng*

#### *1.3.2.3. Quản lý kho hàng*

## 1.4. Các lỗi bảo mật phổ biến trong website TMĐT và cách khắc phục

OWASP là viết tắt của Open Web Application Security Project là một tổ chức phi lợi nhuận quốc tế chuyên về bảo mật ứng dụng web. Một trong những nguyên tắc cốt lõi của OWASP là tất cả các tài liệu của tổ chức đều miễn phí và dễ dàng truy cập trên trang web chính thức http://owasp.org, giúp mọi người đặc biệt là ngành an ninh mạng có thể cải thiện tính bảo mật của ứng dụng web. Các tài liệu OWSAP cung cấp bao gồm tài liệu, công cụ, video và diễn đàn. OWASP được biết đến nhiều nhất qua OWASP Top 10.'

OWASP Top 10 là một báo cáo được cập nhật thường xuyên về các nguy cơ bảo mật đối với bảo mật ứng dụng web, tập trung vào 10 rủi ro/lỗ hổng quan trọng nhất. Báo cáo được tổng hợp bởi một nhóm các chuyên gia bảo mật từ khắp nơi trên thế giới. OWASP đề cập đến Top 10 như một "tài liệu nâng cao nhận thức" và họ khuyến nghị tất cả các công ty nên kết hợp báo cáo này vào các quy trình của họ để giảm thiểu rủi ro bảo mật.

### *1.4.1. SQL Injection*

Lỗi bảo mật SQL Injection là một trong những lỗi phổ biến nhất trong các website TMĐT. Đây là lỗi bảo mật cho phép kẻ tấn công thực hiện các cuộc tấn công vào cơ sở dữ liệu của trang web bằng cách chèn các câu lệnh SQL độc hại vào các trường đầu vào trên trang web.

Khi khai thác lỗi SQL Injection, kẻ tấn công có thể truy xuất và thay đổi dữ liệu trong cơ sở dữ liệu của trang web, thực hiện các hoạt động xóa hoặc thêm mới dữ liệu, và thậm chí kiểm soát toàn bộ trang web.

Để ngăn chặn lỗi bảo mật SQL Injection, trang web TMĐT cần áp dụng các biện pháp bảo mật sau:

- Sử dụng các phương pháp mã hóa và xác thực đầu vào đúng cách để gói gọn các nguy cơ tấn công SQL Injection.
- Tạo ra các quy tắc xác thực đầu vào cụ thể để ngăn chặn việc nhập liệu không hợp lệ từ người dùng.
- Áp dụng các biện pháp bảo vệ server như firewalls, antivirus và các biện pháp bảo vệ thông qua giải pháp phần mềm bảo mật.

- Sử dụng các công cụ kiểm tra lỗ hổng bảo mật để tìm ra các lỗ hổng bảo mật trong trang web TMĐT và khắc phục chúng kịp thời.
- Cập nhật và nâng cấp hệ thống thường xuyên, đặc biệt là các thành phần quan trọng như hệ điều hành, phần mềm máy chủ và các ứng dụng trên trang web TMĐT.

Với những biện pháp bảo mật trên, trang web TMĐT sẽ giảm thiểu được rủi ro bị tấn công SQL Injection và đảm bảo an toàn cho khách hàng trong quá trình giao dịch mua bán sản phẩm trên trang web.

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.

### *1.4.2. Cross-Site Scripting (XSS)*

Lỗi bảo mật Cross-Site Scripting (XSS) là một trong những lỗi phổ biến trong các website TMĐT. XSS xảy ra khi kẻ tấn công chèn mã độc, ví dụ như JavaScript, vào trang web và khiến nó được thực thi trên trình duyệt của người dùng.

Khi khai thác lỗi XSS, kẻ tấn công có thể lấy được thông tin cá nhân của người dùng, thực hiện các hành động thay đổi nội dung trang web, hoặc thậm chí điều khiển trang web để thực hiện các hoạt động phi pháp.

Để ngăn chặn lỗi bảo mật XSS, trang web TMĐT cần áp dụng các biện pháp bảo mật sau:

- Sử dụng các phương pháp mã hóa và xác thực đầu vào đúng cách để gói gọn các nguy cơ tấn công XSS.
- Tạo ra các quy tắc xác thực đầu vào cụ thể để ngăn chặn việc nhập liệu không hợp lệ từ người dùng.
- Áp dụng các biện pháp bảo vệ server như firewalls, antivirus và các biện pháp bảo vệ thông qua giải pháp phần mềm bảo mật.
- Sử dụng các công cụ kiểm tra lỗ hổng bảo mật để tìm ra các lỗ hổng bảo mật trong trang web TMĐT và khắc phục chúng kịp thời.

- Cập nhật và nâng cấp hệ thống thường xuyên, đặc biệt là các thành phần quan trọng như hệ điều hành, phần mềm máy chủ và các ứng dụng trên trang web TMĐT.
- Sử dụng HTTPOnly cookies để ngăn chặn việc truy cập cookie trong trình duyệt của người dùng.

### *1.4.3. Cross-Site Request Forgery (CSRF)*

Cross-Site Scripting xảy ra khi các ứng dụng web cho phép người dùng thêm code tùy chỉnh vào đường dẫn url hoặc vào một trang web mà những người dùng khác sẽ nhìn thấy. Lỗ hổng này có thể bị khai thác để chạy mã JavaScript độc hại (malicious JavaScript code) trên trình duyệt của nạn nhân. Ví dụ: kẻ tấn công có thể gửi email cho nạn nhân có vẻ là từ một ngân hàng đáng tin cậy, với một liên kết đến trang web của ngân hàng đó. Tuy nhiên, liên kết này có thể có một số mã JavaScript độc hại được gắn thẻ vào cuối url. Nếu trang web của ngân hàng không được bảo vệ thích hợp chống lại Cross-Site Scripting, thì mã độc hại đó sẽ được chạy trong trình duyệt web của nạn nhân khi họ nhấp vào liên kết.

Các chiến lược giảm thiểu tấn công Cross-Site Scripting bao gồm thoát các yêu cầu HTTP không đáng tin cậy cũng như xác thực và / hoặc loại bỏ các nội dung do người dùng thêm vào. Sử dụng các web development frameworks hiện đại như ReactJS và Ruby on Rails cũng cung cấp một số tính năng bảo vệ khỏi các cuộc tấn công Cross-Site Scripting.

### *1.4.4. Broken Authentication*

Các lỗ hổng trong hệ thống xác thực (login) có thể cho phép kẻ tấn công truy cập vào tài khoản người dùng và thậm chí có khả năng xâm nhập toàn bộ hệ thống bằng tài khoản quản trị viên. Ví dụ: kẻ tấn công có thể lấy một danh sách chứa hàng nghìn tổ hợp tên người dùng / mật khẩu đã biết có được trong một lần vi phạm dữ liệu và sử dụng tập lệnh để thử tất cả các tổ hợp đó trên hệ thống đăng nhập để xem có tổ hợp nào hoạt động không.

Một số chiến lược để giảm thiểu lỗ hổng xác thực là sử dụng xác thực 2 yếu tố two-factor authentication (2FA) cũng như hạn chế hoặc trì hoãn các nỗ lực đăng nhập lặp lại bằng cách sử dụng giới hạn về số lần đăng nhập & thời gian giãn cách giữa các lần đăng nhập sai.

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 kĩ trước khi thực hiện.

#### *1.4.5. Injection Flaw*

## 1.5. Giải pháp xác thực an toàn bảo mật cho dữ liệu và thanh toán

#### *1.5.1. SSL - Secure Socket Layer*

#### *1.5.2. Tokenization*

#### *1.5.3. 3D Secure*

#### *1.5.4. PCI DSS Compliance*

#### *1.5.5. OAuth*

#### *1.5.6. Secure Payment Protocols*

## 1.6. Kết chương

# CHƯƠNG 2. PHÂN TÍCH VÀ THIẾT KẾ WEBSITE TMĐT

## 2.1. Mô tả bài toán

Quá trình phân tích và thiết kế website TMĐT bao gồm các bước sau:

- Phân tích yêu cầu: Đây là bước đầu tiên trong quá trình phát triển trang web TMĐT. Trong bước này, nhóm phân tích cần xác định yêu cầu của khách hàng về tính năng và giao diện của trang web TMĐT. Các yêu cầu này sẽ được sử dụng để tạo ra một kế hoạch phát triển chi tiết cho trang web TMĐT.
- Thiết kế giao diện: Sau khi xác định yêu cầu của khách hàng, nhóm thiết kế sẽ bắt đầu thiết kế giao diện cho trang web TMĐT. Thiết kế này sẽ bao gồm việc xác định cấu trúc của trang web, bố trí các thành phần trên trang web và thiết kế các mẫu giao diện cho các trang khác nhau.
- Phát triển mã nguồn: Khi đã có thiết kế giao diện, nhóm phát triển sẽ bắt đầu phát triển mã nguồn để tạo ra các tính năng cần thiết cho trang web TMĐT.
- Kiểm thử: Sau khi hoàn tất phát triển, trang web TMĐT sẽ được kiểm thử để đảm bảo rằng các tính năng hoạt động chính xác và không có lỗi.
- Triển khai: Khi đã kiểm tra và hoàn tất, trang web TMĐT sẽ được triển khai trên môi trường sản xuất để khách hàng có thể truy cập và sử dụng.
- Bảo trì và cập nhật: Sau khi triển khai, trang web TMĐT sẽ được bảo trì và cập nhật để đảm bảo rằng các tính năng của trang web luôn hoạt động chính xác và cập nhật với các yêu cầu mới của khách hàng.

## 2.2. Phân tích nghiệp vụ và yêu cầu chức năng

### *2.2.1. Chức năng đăng nhập và đăng ký tài khoản*

Chức năng đăng ký tài khoản cho phép khách hàng có thể tạo một tài khoản mới trên trang web TMĐT. Người dùng cần cung cấp thông tin cá nhân như tên đăng nhập, mật khẩu, địa chỉ email và thông tin liên lạc. Thông tin này sẽ được lưu trữ trong hệ thống của trang web để khách hàng có thể đăng nhập lại vào lần sau.

Chức năng đăng nhập cung cấp cho khách hàng quyền truy cập vào các tính năng và dịch vụ của trang web TMĐT. Người dùng sẽ cần nhập tên đăng nhập và mật khẩu của mình để đăng nhập thành công. Sau khi đăng nhập thành công, khách hàng có thể thực hiện các hoạt động như xem lịch sử giao dịch, sửa đổi thông tin cá nhân, quản lý giỏ hàng và thanh toán đơn hàng.

Ngoài ra, việc có chức năng đăng nhập và đăng ký tài khoản còn giúp cho trang web TMĐT có thể thu thập thông tin về khách hàng để có thể cung cấp các dịch vụ tốt hơn và phù hợp với nhu cầu của từng khách hàng.

### *2.2.2. Chức năng tìm kiếm sản phẩm*

Chức năng tìm kiếm sản phẩm cho phép người dùng nhập từ khóa tìm kiếm vào ô tìm kiếm và sau đó hiển thị các sản phẩm liên quan đến từ khóa tìm kiếm đó. Nếu có quá nhiều sản phẩm được tìm thấy, trang web TMĐT có thể sắp xếp chúng theo các tiêu chí khác nhau như giá cả, độ phổ biến, đánh giá của khách hàng hoặc thương hiệu sản phẩm.

Ngoài ra, trang web TMĐT cũng có thể cung cấp các công cụ lọc sản phẩm để giúp khách hàng thu hẹp phạm vi tìm kiếm của mình và tìm kiếm các sản phẩm phù hợp với nhu cầu của mình hơn. Các tiêu chí lọc sản phẩm phổ biến bao gồm màu sắc, kích thước, giá cả và thương hiệu.

Chức năng tìm kiếm sản phẩm cùng với các công cụ lọc sản phẩm giúp khách hàng dễ dàng tìm kiếm các sản phẩm mà họ đang quan tâm và giúp trang web TMĐT cung cấp cho khách hàng những trải nghiệm mua sắm thân thiện và tiện lợi.

### *2.2.3. Chức năng giỏ hàng và thanh toán*

Chức năng giỏ hàng cho phép người dùng lưu trữ các sản phẩm mà họ muốn mua vào trong giỏ hàng. Người dùng có thể thêm hoặc xóa bất kỳ sản phẩm nào từ giỏ hàng của mình và có thể xem toàn bộ giỏ hàng của mình trước khi hoàn tất đơn hàng.

Sau khi đã chọn các sản phẩm mua, khách hàng cần thực hiện thanh toán để hoàn tất đơn hàng. Chức năng thanh toán cung cấp cho khách hàng các phương thức thanh toán khác nhau để lựa chọn, bao gồm thanh toán qua thẻ tín dụng/debit, thanh toán COD (thanh toán khi nhận hàng) hoặc chuyển khoản ngân hàng.

Ngoài ra, trang web TMĐT cũng cần đảm bảo rằng các thông tin thanh toán của khách hàng được bảo mật và an toàn. Vì vậy, trang web TMĐT cần sử dụng các công nghệ bảo mật như SSL (Secure Sockets Layer) để mã hóa thông tin thanh toán và tránh các vấn đề bảo mật như lừa đảo hoặc giả mạo thông tin.

Với chức năng giỏ hàng và thanh toán, trang web TMĐT cung cấp cho khách hàng một trải nghiệm mua sắm thuận tiện và an toàn, giúp tăng tính khả thi của quy trình hoàn tất mua hàng và tạo ra sự hài lòng cho người dùng.

### *2.2.4. Chức năng quản lý thông tin tài khoản và đơn hàng*

Chức năng quản lý thông tin tài khoản cho phép khách hàng cập nhật và sửa đổi thông tin cá nhân của mình, bao gồm tên, địa chỉ, số điện thoại và địa chỉ email.

Khách hàng cũng có thể thay đổi thông tin đăng nhập của mình như tên đăng nhập và mật khẩu để bảo mật tài khoản của mình.

Chức năng quản lý đơn hàng cho phép khách hàng xem lại các đơn hàng đã đặt trước đó và theo dõi trạng thái của từng đơn hàng. Khách hàng có thể xem chi tiết về sản phẩm đã đặt, nhà cung cấp, số lượng, giá cả và thông tin vận chuyển. Ngoài ra, khách hàng cũng có thể hủy bỏ đơn hàng hoặc yêu cầu trả lại sản phẩm trong trường hợp sản phẩm không đáp ứng được yêu cầu của khách hàng.

Các chức năng quản lý thông tin tài khoản và đơn hàng giúp người dùng có thể quản lý thông tin của mình một cách dễ dàng và tiện lợi. Đồng thời, chức năng này cũng giúp trang web TMĐT có thêm cơ hội tương tác với khách hàng và cung cấp cho họ các dịch vụ chăm sóc khách hàng tốt nhất.

## 2.3. Thiết kế giao diện và trải nghiệm người dùng

### *2.3.1. Thiết kế giao diện*

### *2.3.2. Trải nghiệm người dùng*

## 2.4. Thiết kế cơ sở dữ liệu

### *2.4.1. Lựa chọn hệ quản trị cơ sở dữ liệu*

### *2.4.2. Thiết kế mô hình dữ liệu*

### *2.4.3. Thiết kế quan hệ giữa các bảng dữ liệu*

### *2.4.4. Thiết kế các truy vấn và thủ tục lưu trữ*

### *2.4.5. Phân tích và tối ưu hóa hiệu suất cơ sở dữ liệu*

### *2.4.6. Đảm bảo tính nhất quán và an toàn cho cơ sở dữ liệu*

## 2.5. Phân tích thiết kế kiến trúc hệ thống

### *2.5.1. Xác định các thành phần của hệ thống*

### *2.5.2. Thiết kế và xây dựng kiến trúc hệ thống*

*2.5.3. Đánh giá hiệu năng và khả năng mở rộng của hệ thống*

*2.5.4. Áp dụng các tiêu chuẩn trong thiết kế kiến trúc hệ thống*

**2.6. Đảm bảo an toàn và bảo mật cho website**

*2.6.1. Sử dụng HTTPS để bảo mật kết nối*

*2.6.2. Xác thực người dùng và quản lý phiên làm việc*

*2.6.3. Kiểm tra dữ liệu đầu vào và đầu ra*

*2.6.4. Áp dụng các giải pháp bảo mật như CAPTCHA, ReCaptcha*

*2.6.5. Theo dõi và giám sát hệ thống thường xuyên*

**2.7. Quản lý và bảo vệ thông tin khách hàng trên website TMĐT**

*2.7.1. Quản lý thông tin cá nhân và dữ liệu khách hàng*

*2.7.2. Bảo vệ thông tin giao dịch trên website TMĐT*

*2.7.3. Các qui định pháp lý liên quan*

**2.8. Kết chương**

# CHƯƠNG 3. XÂY DỰNG SẢN PHẨM

## 3.1. Môi trường phát triển và công nghệ sử dụng

- OS: Linux
- Web hosting control panel: cPanel
- Webserver: Apache
- Version control system: Git, Github
- Front-end: Nuxt, Next, TailwindCSS
- Back-end: Node
- Database: MySQL
- IDE: Visual Studio Code
- Khác: Firebase

## 3.2. Các bước triển khai

### *3.2.1. Chuẩn bị môi trường phát triển*

Việc chuẩn bị môi trường phát triển là rất quan trọng trong quá trình phát triển của một dự án web. Có nhiều yếu tố ảnh hưởng đến việc lựa chọn công nghệ: chi phí, chất lượng nhân lực, tính mở rộng, sự phổ biến và hỗ trợ từ cộng đồng của công nghệ đó,… Việc lựa chọn công nghệ phù hợp với dự án giúp cho việc phát triển dự án nhanh chóng, hiệu quả và ít rủi ro hơn.

Sau nhiều lần tìm hiểu và cân nhắc, em quyết định sử dụng Node, Nuxt, Next đều là các công nghệ phổ biến trong cộng đồng và được cập nhật thường xuyên và đều sử dụng chung ngôn ngữ Javascript/Typescript giúp cho việc bảo trì và tái sử dụng trở nên dễ dàng.

Về IDE thì lựa chọn phổ biến nhất cho lập trình viên web đó là VS Code do đây là IDE được sử dụng phổ biến và được hỗ trợ rất tốt từ cộng đồng với khả năng tùy biến cao và nhiều plugin kèm theo. Ngoài ra còn do cá nhân em đã có nhiều kinh nghiệm sử dụng VS Code. Đây là lựa chọn thuộc về chất lượng nhân lực.

Về phần hạ tầng em chủ trương sử dụng web hosting để tiết kiệm chi phí, do đó đi kèm theo là sử dụng hệ điều hành Linux, cPanel control panel, MySQL database và Apache web server do đây là 4 service kèm theo phổ biến của shared web hosting giá rẻ. Ngoài ra em còn sử dụng Firebase để triển khai phần client front-end cho dự án.

*3.2.2. Thiết kế giao diện và trải nghiệm người dùng*

Em sử dụng hệ thống thiết kế cơ bản của Tailwind làm hệ thống thiết kế chính cho dự án. Tailwind là một thư viện design component phổ biến trong cộng đồng do đó có đa dạng thiết kế và ý tưởng được hỗ trợ từ cộng đồng.

Em cũng dành nhiều thời gian tham gia trải nghiệm các sản phẩm tương tự khác, trong số đó có nhiều sản phẩm phổ biến để đánh giá ưu nhược điểm của trải nghiệm người dùng từ đó cải thiện trải nghiệm cho sản phẩm này.

*3.2.3. Lập trình các chức năng và tính năng*

*3.2.4. Đảm bảo an toàn và bảo mật cho website*

*3.2.5. Triển khai website TMĐT*

## 3.3. Kiểm thử và nâng cao chất lượng sản phẩm

*3.3.1. Kiểm thử chức năng*

*3.3.2. Kiểm thử hiệu suất và tải trang*

*3.3.3. Kiểm thử bảo mật*

*3.3.4. Nâng cao chất lượng sản phẩm*

## 3.4. Quản lý và vận hành website

*3.4.1. Quản lý nội dung website*

*3.4.2. Quản lý danh mục sản phẩm và kho hàng*

*3.4.3. Quản lý đơn hàng và thanh toán*

*3.4.4. Quản lý khách hàng và dịch vụ hỗ trợ*

## 3.5. Kết chương

# CHƯƠNG 4. PHỤ LỤC

## 4.1. Ưu nhược điểm của các website TMĐT

Ưu điểm của các website thương mại điện tử hiện nay:

- Tiết kiệm chi phí: Các website thương mại điện tử không cần thiết kế, xây dựng và duy trì các cửa hàng vật lý, do đó giảm chi phí đầu tư ban đầu và chi phí hoạt động.
- Mở rộng thị trường: Các website thương mại điện tử có khả năng tiếp cận hàng triệu khách hàng trên toàn thế giới, giúp doanh nghiệp mở rộng thị trường và tăng doanh số bán hàng.
- Tăng tính tiện lợi: Khách hàng có thể mua sắm mọi lúc mọi nơi chỉ cần có kết nối internet, đặc biệt là trong bối cảnh dịch bệnh Covid-19 khi việc ra ngoài bị giới hạn.
- Dễ dàng tùy chỉnh và cập nhật: Các website thương mại điện tử cho phép doanh nghiệp dễ dàng tùy chỉnh sản phẩm, giá cả, thông tin khuyến mãi, v.v. và cập nhật liên tục để phù hợp với thị trường và nhu cầu khách hàng.
- Phân tích dữ liệu: Thông qua các công cụ phân tích dữ liệu, các website thương mại điện tử có thể thu thập và phân tích thông tin về hành vi mua sắm của khách hàng, từ đó đưa ra các chiến lược tiếp cận khách hàng hiệu quả.

Tuy nhiên, các website thương mại điện tử cũng có những nhược điểm sau:

- Khả năng bảo mật: Khi giao dịch trực tuyến, khách hàng sẽ chia sẻ thông tin cá nhân và tài khoản ngân hàng, do đó, các website thương mại điện tử phải đảm bảo khả năng bảo mật thông tin.
- Độ tin cậy: Một số khách hàng có thể không tin tưởng vào việc mua hàng trực tuyến, đặc biệt là đối với những doanh nghiệp mới hoặc chưa được đánh giá cao.
- Hạn chế trải nghiệm mua sắm: Khách hàng không thể cầm sản phẩm trực tiếp và kiểm tra chất lượng sản phẩm trước khi mua.
- Vấn đề giao hàng: Việc giao hàng có thể gặp nhiều khó khăn và thời gian giao hàng cũng không được nhanh chóng đối với các sản phẩm có kích thước lớn hoặc cồng kềnh.
- Cạnh tranh khốc liệt: Với số lượng website thương mại điện tử ngày càng tăng, đối thủ cạnh tranh trở nên khốc liệt hơn bao giờ hết, do đó, các doanh nghiệp phải đầu tư nhiều hơn để tiếp cận khách hàng và thu hút sự chú ý của họ.

# CHƯƠNG 5. TÀI LIỆU THAM KHẢO

1. https://vinsep.com/kien-thuc/security/owasp-la-gi-top-10-owasp-la-gi/#Injection
2.