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

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.

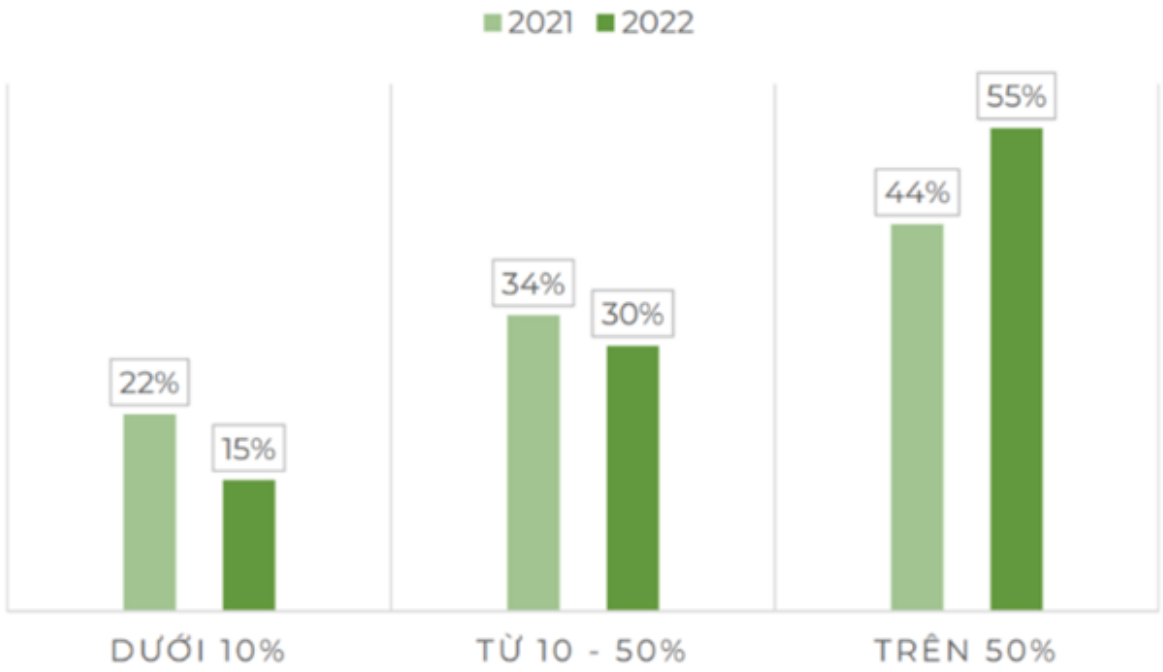
CHƯƠNG 1. CƠ SỞ LÝ THUYẾT

1.1. Tổng quan đề tài

1.1.1. Đặt vấn đề

Theo Hiệp hội Thương mại điện tử Việt Nam, hoạt động kinh doanh trên các sàn thương mại điện tử và mạng xã hội là những nét nổi bật của ngành thương mại điện tử Việt Nam năm 2022 và quý 1/2023. Kết quả khảo sát cho thấy có tới 65% doanh nghiệp đã triển khai hoạt động kinh doanh trên các mạng xã hội.

Ngoài ra, số lượng lao động trong doanh nghiệp thường xuyên sử dụng các công cụ như Zalo, WhatsApp, Viber hay Facebook Messenger cũng liên tục tăng qua từng năm.



Hình 1: Đồ thị người dùng sử dụng các nền tảng Zalo, Facebook ...trong 2 năm

Theo Tổng cục Thống kê, năm 2022 GDP nước ta tăng 8,0%. Trong đó, khu vực dịch vụ được khôi phục và tăng trưởng mạnh mẽ với tốc độ tăng 10,0%. Một số ngành dịch vụ thị trường tăng cao như: ngành bán buôn, bán lẻ tăng 10,2%; ngành vận tải kho bãi tăng 12,0%; ngành dịch vụ lưu trú và ăn uống tăng cao nhất trong khu vực dịch vụ với mức tăng 40,6%…

Tổng mức bán lẻ hàng hóa và doanh thu dịch vụ tiêu dùng năm 2022 ước đạt 5.680 nghìn tỷ đồng với mức tăng trưởng 19,8%, nếu loại trừ yếu tố giá tăng 15,6%.

Sang năm 2023, theo Tổng cục Thống kê, 3 tháng đầu năm tổng sản phẩm trong nước tăng 3,3% so với cùng kỳ năm trước. Trong đó, tổng mức bán lẻ hàng hóa và doanh thu dịch vụ tiêu dùng ước đạt 1.505,3 nghìn tỷ đồng, tăng 13,9% so với cùng kỳ năm trước, nếu loại trừ yếu tố giá tăng 10,3%. Hai ngành dịch vụ tăng trưởng nhanh nhất là dịch vụ lưu trú và ăn uống tăng 26,0%, ngành bán buôn và bán lẻ tăng 8,1%.

Với sự phát triển mang tính toàn cầu của mạng Internet và TMĐT, con người có thể mua bán hàng hoá và dịch vụ thông qua mạng máy tính toàn cầu một cách dễ dàng trong mọi lĩnh vực thương mại rộng lớn . Tuy nhiên đối với các giao dịch mang tính nhạy cảm này cần phải có những cơ chế đảm bảo bảo mật và an toàn vì vậy vấn đề an toàn bảo mật thông tin trong thương mại điện tử là một vấn đề hết sức quan trọng.

Hiện nay vấn đề an toàn bảo mật cho dữ liệu và thanh toán trong TMĐT đã và đang được áp dụng phổ biến và rộng rãi ở Việt Nam và trên phạm vi toàn cầu. Vì thế vấn đề an toàn bảo mật cho dữ liệu và thanh toán đang được nhiều người tập trung nghiên cứu và tìm mọi giải pháp để đảm bảo an toàn bảo mật cho các hệ thống thông tin trên mạng. Tuy nhiên cũng cần phải hiểu rằng không có một hệ thống thông tin nào đợợc bảo mật 100% bất kỳ một hệ thống thông tin nào cũng có những lỗ hổng về bảo mật và an toàn mà chưa được phát hiện ra. Vấn đề an toàn bảo mật thông tin cho dữ liệu và thanh toán trong TMĐT phải đảm bảo bốn yêu cầu sau đây:

- Đảm bảo tin cậy: Các nội dung thông tin không bị theo dõi hoặc sao chép bởi những thực thể không đợợc uỷ thác.
- Đảm bảo toàn vẹn: Các nội dung thông tin không bị thay đổi bởi những thực thể không đợợc uỷ thác.
- Sự chứng minh xác thực: Không ai có thể tự trá hình nhợ là bên hợp pháp trong quá trình trao đổi thông tin.
- Không thể thoái thác trách nhiệm: Ngợời gửi tin không thể thoái thác về những sự việc và những nội dung thông tin thực tế đã gửi đi.

1.1.2. Mục tiêu đề tài

- Xây dựng website TMĐT.
- Tìm hiểu các vấn đề an toàn đối với website TMĐT.
- Triển khai bảo mật cho API server, tìm hiểu giao thức SPP(Secure Payment Protocol).
- Đề tài nghiên cứu các kỹ thuật và triển khai các phương pháp mã hóa bảo vệ dữ liệu, chống xâm nhập và đánh cắp dữ liệu.
- Áp dụng các kết quả đã tìm hiểu và nghiên cứu để triển khai hệ thống an toàn bảo mật cho dữ liệu và thanh toán trong TMĐT.

1.2. Tổng quan về thương mại điện tử

1.2.1. Khái niệm thương mại điện tử

Thương mại điện tử (hay còn gọi là e-commerce, e-comm hay EC) hiểu một cách đơn giản là hoạt động mua bán sản phẩm hay dịch vụ thông qua Internet và các phương tiện điện tử khác. Các giao dịch này gồm tất cả hoạt động như: mua bán, thanh toán, đặt hàng, quảng cáo và giao hàng … Có nhiều tổ chức lớn trên thế giới đưa ra các định nghĩa khác nhau cho khái niệm của thương mại điện tử.

Theo Ủy ban Kinh tế Liên Hiệp Quốc châu Âu (UNECE): "Thương mại điện tử nội địa bao gồm các giao dịch trong nước qua Internet hoặc các mạng máy tính trung gian, trong khi đó, thương mại điện tử quốc tế liên quan đến các giao dịch xuyên biên giới. Các giao dịch này là giao dịch mua/bán hàng hóa hoặc dịch vụ, sau đó, quá trình chuyển giao hàng hóa có thể được thực hiện trực tuyến hoặc thủ công".

Theo Tổ chức Thương mại Thế giới (WTO): "Thương mại điện tử bao gồm việc sản xuất, quảng cáo, bán hàng và phân phối sản phẩm được mua bán và thanh toán trên mạng Internet, nhưng được giao nhận một cách hữu hình, cả các sản phẩm giao nhận cũng như những thông tin số hoá thông qua mạng Internet".

Ngày nay ngươi ta còn hiểu khái niệm Thương mại điện tử thông thường là tất cả các phương pháp tiến hánh kinh doanh và các quy trình quản trị thông qua các kêng điện tử mà trong đó internet đóng vai trò cơ bản và trong công nghệ thông tin được gọi là điều kiện tiên quyết. Một khía cạnh quan trọng khác là không còn phảo thay đổi phương tiện truyền thông, một đặc trưng cho việc tiến hành kinh doanh truyền thống. Thêm vào đó laf thắng đến gia công , để làm điều này đòi hỏi phải tích hợp rộng lớn các tính năng kinh doanh.

Tuy nhiên, thương mại điện tử không chỉ là kinh doanh sử dụng công nghệ. Thương mại điện tử là toàn bộ quá trình kinh doanh được thực hiện bằng điện tử và được thiết kế để giúp hoàn thành mục tiêu kinh doanh. Hai công nghệ chủ chốt để xây dựng và phát triển thương mại điện tử là trao đổi dữ liệu điện tử (EDI) và chuyển tiền điện tử (EFT). Ngày nay, công nghệ chuyển tiền điện tử được ứng dụng để xây dựng các hệ thống thanh toán điện tử.

Website thương mại điện tử (TMĐT) là một nền tảng trực tuyến cho phép các doanh nghiệp bán hàng hoặc dịch vụ của mình cho khách hàng thông qua internet. TMĐT cung cấp một kênh bán hàng trực tuyến, mở rộng phạm vi tiếp cận của doanh nghiệp đến toàn bộ thị trường và giúp tăng thu nhập.

1.2.2. Lợi ích của một trang thương mại điện tử

Website thương mại điện tử (TMĐT) mang lại nhiều lợi ích cho các doanh nghiệp và khách hàng, bao gồm:

- Mở rộng phạm vi tiếp cận khách hàng: TMĐT giúp các doanh nghiệp tiếp cận được với khách hàng từ khắp nơi trên thế giới, không chỉ ở địa phương hay khu vực.
- Tiết kiệm chi phí: So với việc mở cửa hàng truyền thống, TMĐT giảm thiểu chi phí thuê mặt bằng, tài liệu quảng cáo, nhân viên bán hàng…
- Tăng doanh số bán hàng: TMĐT giúp các doanh nghiệp tăng doanh số bán hàng bằng cách thu hút khách hàng mới, tăng số lượng đơn hàng, tăng giá trị các đơn hàng và tối ưu hóa quy trình bán hàng.
- Tăng tính minh bạch trong quản lý kinh doanh: TMĐT cung cấp thông tin về sản phẩm, giá cả, khách hàng, doanh số… giúp các doanh nghiệp quản lý kinh doanh dễ dàng hơn và tăng tính minh bạch trong hoạt động kinh doanh.
- Đáp ứng nhu cầu của khách hàng: Khách hàng có thể dễ dàng tìm kiếm sản phẩm, so sánh giá cả, đặt hàng và thanh toán trực tuyến mà không phải tốn thời gian và chi phí di chuyển.
- Tăng tính tiện lợi cho khách hàng: TMĐT cung cấp các tính năng hỗ trợ khách hàng như chat trực tuyến, điện thoại, email… giúp khách hàng dễ dàng liên hệ với doanh nghiệp khi cần thiết.
- Tiết kiệm thời gian: Khách hàng có thể tìm kiếm sản phẩm và đặt hàng trong vài phút, không cần phải di chuyển đến cửa hàng truyền thống.
- Hỗ trợ quản lý đơn hàng dễ dàng: TMĐT giúp các doanh nghiệp quản lý danh sách đơn hàng và tiến độ giao hàng một cách thuận tiện, giúp tối ưu hóa quy trình bán hàng.

1.2.3. Các đặc trưng cơ bản của thương mại điện tử (TMĐT)

So với các hoạt động thương mại truyền thống, TMĐT có một số các đặc trọng cơ bản sau:

- Truy cập từ xa: Khách hàng có thể truy cập và mua hàng từ bất kỳ nơi đâu, thông qua Internet hoặc các thiết bị kết nối mạng khác.
- Thanh toán trực tuyến: Hình thức thanh toán trực tuyến cho phép khách hàng dễ dàng thanh toán cho các sản phẩm hoặc dịch vụ mà họ đã mua thông qua một số phương thức thanh toán như thẻ tín dụng, chuyển khoản ngân hàng hoặc ví điện tử.
- Mở cửa 24/7: Các trang web TMĐT có thể hoạt động liên tục, 24 giờ một ngày, 7 ngày một tuần, giúp khách hàng có thể mua sắm vào bất kỳ thời điểm nào.

- Phạm vi rộng: TMĐT cho phép các nhà bán hàng tiếp cận đến một số lượng khách hàng rất lớn và có thể bán sản phẩm của họ tới khách hàng ở khắp nơi trên thế giới.
- Tiết kiệm chi phí: Với TMĐT, các nhà bán hàng không cần phải thuê mặt bằng để mở cửa hàng và chi trả các chi phí liên quan đến việc duy trì một cửa hàng thực tế. Họ có thể tiết kiệm chi phí này và đưa giá thành sản phẩm của họ xuống để cạnh tranh.
- Đa dạng sản phẩm: TMĐT cung cấp cho khách hàng một loạt các sản phẩm và dịch vụ khác nhau từ nhiều nhà bán hàng khác nhau. Khách hàng có thể so sánh giá cả và chất lượng sản phẩm để chọn lựa được sản phẩm phù hợp nhất với mình.
- Trải nghiệm người dùng tốt: Các trang web TMĐT cung cấp trải nghiệm người dùng tốt, thuận tiện và dễ sử dụng nhằm giúp khách hàng tìm kiếm sản phẩm một cách nhanh chóng và tiện lợi hơn.

1.2.4. Các loại thị trường điện tử

- Thị trường B2B (Business-to-Business): Thị trường này là nơi các doanh nghiệp kinh doanh với nhau thông qua internet hoặc các kênh truyền thông kỹ thuật số khác. Các sản phẩm và dịch vụ được mua và bán trong thị trường B2B này thường liên quan đến các sản phẩm và dịch vụ cần thiết cho việc sản xuất và kinh doanh của các doanh nghiệp.
- Thị trường B2C (Business-to-Consumer): Đây là loại thị trường điện tử phổ biến nhất, nơi các doanh nghiệp bán hàng trực tiếp cho người tiêu dùng thông qua các trang web TMĐT hoặc các ứng dụng di động. Thị trường B2C này bao gồm một loạt các sản phẩm và dịch vụ từ quần áo, giày dép, đồ gia dụng, đồ điện tử, đồ chơi, sách, tạp chí, sách điện tử và nhiều hơn nữa.
- Thị trường C2C (Consumer-to-Consumer): Thị trường C2C cho phép người tiêu dùng bán hàng cho nhau thông qua các trang web đấu giá hoặc trang web trao đổi sản phẩm. Thị trường này thường bao gồm các sản phẩm như quần áo, giày dép, đồ gia dụng, sách, đồ chơi và các sản phẩm cũ khác.
- Thị trường G2B (Government-to-Business): Thị trường này là nơi các tổ chức công quyền như các cơ quan chính phủ, tổ chức phi chính phủ và các tổ chức công cộng cung cấp các sản phẩm và dịch vụ cho các doanh nghiệp.
- Thị trường G2C (Government-to-Consumer): Thị trường G2C là nơi các tổ chức công quyền cung cấp các thông tin và dịch vụ cho người tiêu dùng thông qua các trang web hoặc ứng dụng di động, ví dụ như thông tin về các chương trình chăm sóc sức khỏe, giấy phép lái xe và các dịch vụ khác.
- Thị trường C2G (Consumer-to-Government): Thị trường này là nơi người tiêu dùng cung cấp thông tin cho các tổ chức công quyền, ví dụ như thông tin cá nhân và thông tin thuế qua các kênh truyền thông kỹ thuật số.

1.2.5. Dữ liệu trong TMĐT

Dữ liệu trong thương mại điện tử (e-commerce) là các thông tin liên quan đến việc mua bán hàng hóa hoặc dịch vụ trực tuyến giữa người tiêu dùng và doanh nghiệp. Dữ liệu này có thể bao gồm:

- Thông tin khách hàng: Bao gồm thông tin cá nhân của khách hàng, thông tin địa chỉ, thông tin thanh toán, lịch sử mua hàng của khách hàng và các thông tin khác liên quan đến hành vi mua hàng trực tuyến.
- Thông tin sản phẩm: Gồm thông tin về sản phẩm, giá cả, số lượng, đặc tính kỹ thuật, hình ảnh, video, đánh giá từ người dùng và các thông tin khác liên quan đến sản phẩm.
- Lưu lượng truy cập: Các thông tin về lượt truy cập trang web, giờ và ngày truy cập, các trang được truy cập nhiều nhất và các thông tin khác về hành vi của người dùng trên trang web.
- Dữ liệu hệ thống: Bao gồm các thông tin liên quan đến hệ thống máy chủ, thiết bị và phần mềm được sử dụng để quản lý và vận hành trang web.

Dữ liệu trong thương mại điện tử là rất quan trọng, vì nó giúp các doanh nghiệp cung cấp dịch vụ và sản phẩm phù hợp với nhu cầu của khách hàng, cải thiện trải nghiệm mua hàng trực tuyến và tối ưu hóa hoạt động kinh doanh của mình. Tuy nhiên, việc quản lý và bảo vệ dữ liệu này cũng là một thách thức đối với các doanh nghiệp, vì có rất nhiều thông tin nhạy cảm liên quan đến khách hàng và sản phẩm.

1.2.6. Các hệ thống thanh toán trong TMĐT

Có nhiều hệ thống thanh toán được sử dụng trong thương mại điện tử (TMĐT), bao gồm:

- Thanh toán trực tiếp (Direct Payment): Đây là phương thức thanh toán được thực hiện trực tiếp trên trang web TMĐT với các công cụ thanh toán như thẻ tín dụng, thẻ ghi nợ, ví điện tử hoặc chuyển khoản ngân hàng.
- Thanh toán qua cổng thanh toán (Payment Gateway): Các cổng thanh toán là các bên trung gian cho phép khách hàng thanh toán trực tuyến thông qua các phương thức thanh toán như thẻ tín dụng, chuyển khoản ngân hàng hoặc ví điện tử. Các cổng thanh toán thông dụng như PayPal, Stripe, và 2Checkout.
- Thanh toán khi nhận hàng (Cash on Delivery - COD): Đây là phương thức được sử dụng phổ biến tại các quốc gia đang phát triển, khách hàng chỉ thanh toán tiền mặt khi nhận hàng.
- Thanh toán bằng ví điện tử (E-wallet): Đây là phương thức thanh toán mới nhất, cho phép khách hàng liên kết tài khoản ngân hàng của họ với một ví điện tử để

thanh toán trên trang web TMĐT. Các ví điện tử phổ biến như PayPal, Google Wallet và Apple Pay.

- Thanh toán qua Internet Banking: Đây là phương thức thanh toán được sử dụng để chuyển khoản tiền từ tài khoản ngân hàng của khách hàng cho doanh nghiệp bán hàng trực tuyến.
- Thanh toán qua mã QR: Đây là phương thức thanh toán mới ra đời, thông qua việc quét mã QR trên sản phẩm hoặc trang web TMĐT để thanh toán thông qua tài khoản ví điện tử.

Các hình thức thanh toán trên TMĐT được thiết kế để mang lại sự tiện lợi và an toàn cho khách hàng khi mua sắm trực tuyến.

1.2.6.1. Công nghệ thanh toán điện tử

Thanh toán điện tử hay thanh toán trực tuyến là một mô hình giao dịch không sử dụng tiền mặt được thực hiện trên môi trường internet. Thông qua hệ thống thanh toán điện tử, người sử dụng có thể thực hiện các hoạt động thanh toán, chuyển, nạp hay rút tiền, …

Thông thường, thanh toán điện tử được thực hiện qua các cổng thanh toán trực tuyến (giữ vai trò trung gian thực hiện các giao dịch lưu chuyển tiền tệ trực tuyến, có sự liên kết với các ngân hàng thương mại) hoặc các tài khoản ngân hàng trực tuyến của người dùng.

Công nghệ thanh toán điện tử là hình thức thanh toán mà người dùng sử dụng các thiết bị công nghệ để thực hiện việc chuyển tiền hoặc thanh toán cho sản phẩm hoặc dịch vụ một cách nhanh chóng và thuận tiện. Các hình thức thanh toán điện tử bao gồm thẻ tín dụng, ví điện tử, thông qua các ứng dụng trên điện thoại thông minh, internet banking, thanh toán qua QR code, NFC (Near Field Communication), Smart Contract,…

Công nghệ này đã được phát triển rất mạnh mẽ trong những năm gần đây, đặc biệt là trong bối cảnh dịch bệnh COVID-19 khi các khoản thanh toán trực tuyến trở nên phổ biến hơn bao giờ hết. Thanh toán điện tử mang lại nhiều tiện ích cho người dùng như tiết kiệm thời gian, an toàn và tiết kiệm chi phí.

1.2.6.2. Các phương thức thanh toán điện tử hiện nay

Một số hình thức thanh toán điện tử được sử dụng rộng rãi trong các hệ thống thanh toán điện tử được trình bày dưới đây:

- Thanh toán bằng thẻ: Đây là hình thức thanh toán đặc trưng nhất, chiếm tới 90% trong tổng số các giao dịch thanh toán điện tử. Thẻ thanh toán (thẻ chi trả) là một

loại thẻ có khả năng thanh toán tiền mua hàng hóa, dịch vụ tại một vài địa điểm, kể cả website mua hàng trực tuyến nếu chấp nhận tiêu dùng bằng thẻ đó. Thẻ có thể dùng để rút tiền mặt trực tiếp từ các ngân hàng hay các máy rút tiền tự động.

- Thanh toán qua cổng thanh toán điện tử: Cổng thanh toán điện tử về bản chất là dịch vụ cho phép khách hàng giao dịch tại các website thương mại điện tử. Cổng thanh toán cung cấp hệ thống kết nối an toàn giữa tài khoản (thẻ, ví điện tử,…) của khách hàng với tài khoản của website bán hàng. Cổng thanh toán điện tử giúp người tiêu dùng và doanh nghiệp thanh toán, nhận tiền trên internet đơn giản, nhanh chóng và an toàn.
- Thanh toán bằng ví điện tử: Ví điện tử là một tài khoản online có thể dùng nhận, chuyển tiền, mua thẻ điện thoại, vé xem phim, thanh toán trực tuyến các loại phí trên internet như tiền điện nước, cước viễn thông, cũng có thể mua hàng online từ các trang thương mại điện tử. Người dùng phải sở hữu thiết bị di động thông minh tích hợp ví điện tử và liên kết với ngân hàng thì mới có thể thanh toán trực tuyến bằng hình thức này.
- Thanh toán bằng thiết bị điện thoại thông minh:
  - Thanh toán qua Mobile Banking: Hình thức này đang dần trở nên phổ biến bởi hầu hết người dùng đều sử hữu một chiếc điện thoại thông minh. Chính vì vậy, khi đi mua sắm, khách hàng không cần phải mang theo tiền mặt, thay vào đó là thanh toán qua điện thoại với dịch vụ Mobile Banking. Hệ thống thanh toán qua điện thoại được xây dựng trên mô hình liên kết giữa ngân hàng, các nhà cung cấp viễn thông, và người dùng.
  - Thanh toán qua QR Code: Tiến bộ công nghệ cũng là lý do khiến thanh toán bằng QR Code ngày càng được ưa chuộng. Phương thức thanh toán này khá đơn giản, gọn nhẹ, dễ sử dụng và thân thiện cho người dùng. Tính năng QR Code hiện đang được tích hợp sẵn trên ứng dụng di động của các ngân hàng, các sản phẩm và dịch vụ của Google như Google Chart hay Google Map, trên bảng hiệu, xe buýt, danh thiếp, tạp chí, website, hàng hóa tại siêu thị, cửa hàng tiện lợi,… Thậm chí là trên một số siêu ứng dụng như VinID của Tập đoàn Vingroup. Người dùng sử dụng camera điện thoại quét mã QR để thực hiện nhanh các giao dịch chuyển khoản, thanh toán hóa đơn, mua hàng. Chỉ với một lần quét, sau vài giây, người dùng đã thanh toán thành công tại các nhà hàng, siêu thị, cửa hàng tiện lợi, taxi, thậm chí là các website thương mại điện tử hay trên bất cứ sản phẩm nào có gắn mã QR mà không cần sử dụng tiền mặt, thẻ, không lo lộ thông tin cá nhân tại các điểm thanh toán.

1.2.6.3. Quy trình thanh toán điện tử

Các hệ thống thanh toán điện tử triển khai trong thực tế rất đa dạng về hình thức và công nghệ sử dụng. Hình 1.1 dưới đây trình bày mô hình chung cho một hệ thống thanh toán điện tử.

Hình 2: Quy trình thanh toán điện tử

Trong mô hình trên, hệ thống thanh toán điện tử là trung gian kết nối giữa người mua, người bán, thực hiện thanh toán cho các giao dịch dựa trên kết nối với ngân hàng của người mua và người bán:

1. Thẻ tín dụng: Các khách hàng có thẻ tín dụng do ngân hàng phát hành với hạn mức tín dụng và số dư có sẵn.
2. Đặt hàng: Các khách hàng đến thăm một trang web hoặc cửa hàng trực tuyến sử dụng trình duyệt web tiêu chuẩn và bắt đầu mua sắm và thêm (các) sản phẩm

vào giỏ hàng của mình. Sau khi kiểm tra, người mua được yêu cầu để gửi thông tin thẻ tín dụng của mình, ngày hết hạn, địa chỉ thanh toán. Sau đó, người mua cũng chọn phương thức vận chuyển cho ví dụ và sau đó nhấn vào nút gửi để bắt đầu giao dịch. Các thông tin này sau đó được chuyển đến cửa hàng trực tuyến của thương gia nơi mà các dịch vụ thanh toán bên ngoài được thiết lập. Các dịch vụ thanh toán bên ngoài nhận được thông tin được mã hóa từ các cửa hàng trực tuyến, thực hiện một kiểm tra gian lận, và sau đó bắt đầu quá trình giao tiếp thông tin thanh toán và số tiền mua hàng cho các bộ xử lý của bên thứ ba.

3. Yêu cầu xác nhận: Dịch vụ dịch thanh toán mã hóa thông tin mua hàng hoặc dữ liệu và truyền nó cho các bộ xử lý của bên thứ ba, người sẽ chuyển thông tin hoặc dữ liệu hơn nữa để các hiệp hội thẻ hoặc thẻ phát hành cho phép và xác minh
4. Đáp trả xác thực: Các tổ chức tài chính phát hành xác minh thông tin thẻ tín dụng và xác định xem khách hàng có đủ tín dụng để thanh toán tiền mua. Một số quyền được tạo ra và tín dụng là giảm lượng có thẩm quyền. Nếu nó để xảy ra rằng các thông tin thẻ tín dụng là không đúng hoặc nếu không có đủ tín dụng có sẵn, sau đó nhắn giảm giao dịch được tạo ra. Trong khoảng thời gian ngắn này của thời gian, các ngân hàng phát hành cũng thực hiện các hoạt động khác như dịch vụ xác minh địa chỉ, nơi các thông tin thanh toán đã nhập trực tuyến được so sánh với các mục trong cơ sở dữ liệu của ngân hàng phát hành - đây là phần xác thực. Sau đó, một thông báo uỷ quyền được trả lại cho các hiệp hội thẻ và chuyển tiếp đến các bộ xử lý của bên thứ ba.
5. Thông báo cho bên bán: Bộ xử lý của bên thứ ba nhận được tin nhắn uỷ quyền và các thông tin cần thiết khác từ các hiệp hội thẻ hoặc tổ chức phát hành và khởi tạo quá trình truyền đạt thông điệp uỷ quyền cho các thương gia. Các bộ vi xử lý của bên thứ ba mã hóa thông điệp uỷ quyền và truyền các thông tin mã hóa cho máy chủ thương mại an toàn của bên bán.
6. Thông báo từ bên bán: máy chủ của bên bán thu được các thông tin và được lập trình để gửi ngay cho chính người mua hoặc tin nhắn cho chủ thẻ/khách hàng. Thông thường khi thẻ tín dụng bị từ chối, một số thông tin cần thiết như một gợi ý để kiểm tra tính chính xác của các thông tin được cung cấp hoặc sử dụng một thẻ tín dụng khác để gửi lên. Ngay sau khi khách hàng nhận được thông tin này sẽ đồng ý chấp thuận một giao dịch, cùng một lúc nhận được một số xác nhận. Nó chỉ mất một vài giây từ thời điểm khách hàng nhấn vào nút mua cho đến khi khách hàng nhận được tin nhắn phản hồi trở lại. Các quá trình cấp phép thường mất một vài giây, tùy thuộc vào ứng dụng của bên bán thanh toán và thủ tục cũng như lưu lượng Internet và các yếu tố khác.
7. Hoàn thành: Bên bán bắt đầu quá trình thực hiện lệnh của khách hàng với các sản phẩm/dịch vụ thích hợp.

8. Yêu cầu giải quyết: Các bên bán biên soạn một loạt các đơn đặt hàng đã được hoàn thành và bắt đầu quá trình truyền tải hàng loạt các bộ xử lý của bên thứ ba để giải quyết. Bên bán đầu tiên truyền hàng loạt dịch vụ thanh toán của mình để mã hoá thông tin mua hàng và truyền các thông tin mã hóa cho các bộ vi xử lý của bên thứ ba. Các bộ xử lý của bên thứ ba nhận được thông tin này và sẽ gửi các hướng dẫn giải quyết cho tổ chức tài chính của mình để chuyển số tiền từ tài khoản của chủ thẻ vào tài khoản của thương gia.
9. Giải quyết: Đối với mỗi giao dịch thẻ tín dụng trong hàng loạt, các tổ chức tài chính thích hợp được ghi nợ và thẻ tín dụng của chủ thẻ được cập nhật. Các ngân hàng bên mua nhận tiền và tiền được gửi vào tài khoản ngân hàng của bên bán.
10. Đáp ứng giải quyết: Bên bán nhận được thông báo rằng tiền đã được gửi vào tài khoản ngân hàng của mình. Trên cơ sở đó, các thương gia nhận được báo cáo rằng ông có thể sử dụng để hòa giải với yêu cầu giải quyết hàng loạt của mình với hoạt động tiền gửi của mình.
11. Quỹ có sẵn: Khoảng cách giữa các cấp của thương gia được yêu cầu thanh toán, chuyển tiền và các quỹ sẵn có thể mất đến vài ngày, tùy thuộc vào các ngân hàng phát hành, các ngân hàng mua lại và các bộ xử lý của bên thứ ba. Chu kỳ thời gian giải quyết là thực sự bị ảnh hưởng bởi thời gian nắm giữ ngân hàng mua lại tiền gửi, cũng như các thủ tục khác và chính sách được thiết lập bởi các ngân hàng mua lại và xử lý của bên thứ ba.

1.3. Các yếu tố quan trọng trong thiết kế website TMĐT

1.3.1. Trải nghiệm người dùng (User Experience - UX)

Website bán hàng của bất kỳ doanh nghiệp nào cũng được xem là phương tiện quan trọng để kết nối được với nhiều khách hàng. Vì vậy, chú trọng vào trải nghiệm người dùng (UX) là điều nên làm để giúp khách hàng có được trải nghiệm tốt nhất tại website của bạn. Vậy cách tối ưu trải nghiệm người dùng website thế nào cho hiệu quả, cùng đọc bài viết dưới đây nhé.

Trải nghiệm người dùng (UX) là trải nghiệm của người dùng khi tương tác với một sản phẩm hoặc dịch vụ. Nó bao gồm các khía cạnh như thẩm mỹ, tính tiện dụng, tính khả dụng, hiệu suất và thỏa mãn sử dụng.

Mục đích chính của UX là cải thiện tương tác giữa người dùng và sản phẩm hoặc dịch vụ, từ đó tạo ra trải nghiệm tốt hơn cho người dùng và đẩy mạnh doanh số bán hàng. Để đạt được điều này, các chuyên gia UX thường phân tích và tối ưu hóa các yếu tố như thiết kế giao diện người dùng, quy trình tương tác và trải nghiệm

người dùng tổng thể để đảm bảo rằng sản phẩm hoặc dịch vụ đáp ứng được nhu cầu và mong muốn của người dùng.

Các yếu tố quan trọng khi thiết kế trải nghiệm người dùng:

- Tâm lý người dùng (Psychology): Là một trong những yếu tố quan trọng nhất nhưng cũng phức tạp nhất mà bạn cần có cái nhìn chi tiết để hiểu rõ nó. Khi thiết kế trải nghiệm người dùng, bạn cần phải gạt bỏ những định kiến và ý kiến của bản thân.
- Tính khả dụng (Usability): Tâm lý người thuộc về tiềm thức còn tính khả dụng mang tính chủ quan và nghiêng về ý thức nhiều hơn.Người dùng sẽ có thể thực hiện được các thao tác một cách dễ dàng và nhanh chóng hơn khi tính khả dụng được tối ưu.
- Thiết kế 960px, nhưng chắc chắn nó sẽ hiển thị trên màn hình điện thoại theo chiều rộng là 320px – 420px, đấy (Design): Thiết kế trải nghiệm người dùng không giống với thiết kế trong suy nghĩ của các designer. Với UX, thiết kế này không liên quan quá nhiều đến "phong cách", thay vào đó là thiết kế nguyên lý hoạt động nhiều hơn.
- Sáng tạo nội dung (Copywriting): Khác với nội dung của UX, sáng tạo nội dung Copywriting cho thương hiệu cần phải có sự mạch lạc, rõ ràng, trực quan và đơn giản những nội dung của thương hiệu với mục đích phục vụ cho những giá trị lợi ích và hình ảnh của công ty.
- Phân tích số liệu (Analytics): Phân tích số liệu Analytics tuy là điểm yếu của hầu hết tất cả các designer song điều này có thể khắc phục và cải thiện được. Đây chính là điều kiện chính để giúp phân biệt được thiết kế UX với những thiết kế khác tạo nên điểm mạnh của UX.

1.3.2. Thiết kế responsive

1.3.2.1. Responsive là gì?

Responsive là một thuật ngữ hay tính từ chỉ một website có thể hiển thị và tương thích với mọi trình duyệt (co dãn theo kích thước trình duyệt). Ví dụ thông thường một website có độ hiển thị chuẩn trên màn hình máy tính ở Việt Nam làlà so với những chiếc điện thoại màn hình nhỏ, còn với những chiếc điện thoại lớn hơn thì sẽ hiển thị khác.

Cách thức hoạt động của Responsive là chúng ta sẽ viết code CSS để cho trình duyệt hiểu và thực thi nó trên các kích thước trình duyệt nhất định. Chẳng hạn các bạn có thể code và thiết lập một đoạn CSS nào đó chỉ áp dụng cho các trình duyệt có kích thước chiều rộng tối đa ở Iphone 4 là 640px. Responsive sử dụng kỹ thuật thiết kế được xử lý từ client-side chứ không thông qua truy vấn đến máy chủ để xử

lý (server – side) nên nó có một nhược điểm là làm trình duyệt của bạn phải tốn thời gian chờ đợi để xử lý CSS.

1.3.2.2. Tại sao Responsive Web Design lại quan trọng trong thiết kế web?

- Đáp ứng nhu cầu thực tế

Với sự bùng nổ của sự phát triển các thiết bị di động, người dùng smartphone ngày càng tăng trưởng một cách nhanh chóng. Theo số liệu của We Are Social về người dùng Internet vào 01/2017, thì có hơn 50% sử dụng các thiết bị di động để truy cập Internet. Riêng tại Việt Nam, số lượng này vào khoảng hơn 30% và con số này đang tăng mỗi năm. Như vậy, nhu cầu sử dụng Internet nói chung ngày càng tăng và đặc biệt là có một lượng lớn người dùng truy cập Internet từ thiết bị di động. Vì thế, áp dụng RWD chính là đang đáp ứng với nhu cầu thực tế.

- Hiệu quả kinh tế responsive là gì?

Trước đây, các nhà phát triển phải xây dựng ít nhất hai giao diện cho trang web. Một dành cho PC, một dành cho di động. Hoặc thậm chí một số nhà phát triển còn phải xây dựng ứng dụng mobile. Điều này gây tốn kém về mặt chi phí. Chưa kể trên các ứng dụng hoặc giao diện riêng, việc hiển thị dữ liệu chưa chắc đã giống nhau. Vì thế nhà phát triển có thể gặp khó khăn trong việc quản lý.

Đối với RWD, với nguyên lý là một mã nguồn nhưng đa giao diện, tương thích tốt trên nhiều thiết bị. Mặc dù chúng ta không thể lường trước được kích thước của thiết bị. Nhưng với RWD, chuyện này là hoàn toàn khả thi. Từ đó tiết kiệm công sức và chi phí cho nhà phát triển.

- Được Google Search khuyến khích, lợi ích cho SEO:

Từ năm 2015, Google Search ưu tiên hiển thị các trang web có giao diện RWD. Thay đổi này với mong muốn các trang web hướng tới người dùng hơn. Với mong muốn các kết quả tìm được sẽ có nội dung văn bản dễ đọc hơn. Để kiểm tra, các bạn có thể vào trang Mobile-Friendly Test và nhập URL trang web. Kết quả hiển thị sẽ cho biết mức độ thân thiện của website. Nếu website không thân thiện với di động, thứ hạng trang có thể giảm đáng kể. Một khi trang web hỗ trợ RWD, cụ thể là thân thiện với di động, thứ hạng sẽ được tái xử lý.

- Sử dụng công nghệ tuy mới mà "cũ" responsive là gì?

Đối với Web Developer, thì đây là một thách thức nhưng không phải là không làm được. Tuy gọi là công nghệ mới nhưng RWD cơ bản chỉ áp dụng công nghệ CSS3, cụ thể là Media Query. Nghĩa là nếu trước đó đã tìm hiểu HTML & CSS thì việc này là hoàn toàn nằm trong tầm tay. Đặc biệt, RWD là một trong những khóa học

nằm trong gói lộ trình Thiết Kế Web đang được CiOne cung cấp. Vì thế hãy yên tâm là các bạn sẽ dễ dàng làm chủ được kỹ thuật này một cách có hệ thống.

1.3.2.3. Lợi ích của Responsive Web Design

Từ phần trước, rõ ràng là thiết kế web đáp ứng rất quan trọng đối với bất kỳ trang web nào và việc không tuân thủ có thể dẫn đến thiệt hại tài chính (do giảm lưu lượng truy cập không phải trả tiền vào trang web).

Dưới đây là một số lợi ích chính của Responsive Web Design:

- Cải thiện trải nghiệm người dùng: Nói một cách dễ hiểu, Responsive Web Design mang lại trải nghiệm người dùng mượt mà hơn. Bạn có thể tự kiểm tra xem thiết kế nào trong các màn hình dưới đây cung cấp trải nghiệm người dùng tốt hơn. Trải nghiệm di động tốt là một trong những điều cơ bản nhất cần ghi nhớ khi thiết kế một trang web tuân theo các nguyên tắc Responsive Web Design.
- Hiệu quả về chi phí: Trước khi Responsive Web Design và tương ứng của nó ra đời, các doanh nghiệp dựa vào việc thiết kế các trang web riêng biệt để phục vụ cho các khung nhìn di động khác nhau. Ở đây, một trang chủ tùy chỉnh đã được hiển thị cho người dùng dựa trên thiết bị mà từ đó yêu cầu được thực hiện. Đây không phải là một cách tiếp cận có thể mở rộng vì nó sẽ liên quan đến các sửa đổi trong việc triển khai mỗi khi một thiết bị mới được giới thiệu trên thị trường. Khái niệm này đã được sử dụng trước khi cuộc cách mạng di động đạt được động lực! Tạo một trang web đáp ứng phục vụ cho các chế độ xem, trình duyệt và hệ điều hành khác nhau không còn là một lựa chọn mà là một sự bắt buộc đối với các doanh nghiệp để phát triển trong môi trường siêu cạnh tranh này.
- Tỷ lệ thoát và thời gian phiên: Ngoài chi phí phát triển trang web, Responsive Web Design giúp tiết kiệm tiền và mang lại sự gắn bó cho người dùng. Điều này lần lượt giúp tăng thời gian phiên và giảm tỷ lệ thoát. Cả hai yếu tố này đều ảnh hưởng đến thứ hạng của công cụ tìm kiếm. Theo như các bot của công cụ tìm kiếm được xem xét, chúng không phải là con người có thể đọc và đánh giá nội dung. Nhưng, họ dựa vào con người để làm điều đó. Một trang web có tỷ lệ thoát cao liên tục và thời gian phiên thấp hơn là một chỉ báo cho thấy mọi người không đặc biệt thích trang web đó. Điều này dẫn đến thứ hạng thấp hơn, lưu lượng truy cập ít bị ràng buộc hơn và giảm doanh thu.
- Giảm nỗ lực bảo trì: Các trang web đáp ứng dễ duy trì hơn vì chỉ có một trang web duy nhất mà trên đó các thay đổi được thực hiện để cung cấp cho các thiết bị mới hơn. Tiếp thị và quản lý doanh nghiệp cho sự hiện diện trực tuyến trở nên cực kỳ dễ dàng vì bạn có một trang web duy nhất.
- Trang web Di động riêng biệt: Một thay thế cho thiết kế đáp ứng là phát triển một trang web di động riêng biệt. Cách tiếp cận này có thể giống như quay ngược thời

gian. Với sự ra đời của Responsive Web Design, một trang web duy nhất đã trở thành trọng tâm chính của hầu hết các doanh nghiệp.

1.3.3. Tối ưu hóa tốc độ load trang

Tối ưu hóa tốc độ load trang là một trong những yếu tố quan trọng để cải thiện trải nghiệm người dùng và tăng tương tác trên website của bạn. Dưới đây là một số cách để tối ưu hóa tốc độ load trang:

- Tối ưu hóa hình ảnh: Sử dụng các công cụ tối ưu hóa hình ảnh để giảm dung lượng của các hình ảnh trên trang web của bạn, đồng thời áp dụng kỹ thuật lazy loading để chỉ tải hình ảnh khi cần thiết.
- Sử dụng cache: Sử dụng bộ nhớ cache để giảm thời gian tải lại trang web và cải thiện trải nghiệm người dùng.
- Giảm số lượng yêu cầu HTTP: Giảm số lượng yêu cầu HTTP bằng cách sử dụng các kỹ thuật như gộp file CSS và JavaScript hoặc sử dụng các CDN (Content Delivery Network) để phân phối tài nguyên trên nhiều máy chủ.
- Chọn hosting tốt: Lựa chọn một nhà cung cấp hosting tốt có thể giúp tăng tốc độ tải trang web của bạn.
- Tối ưu hóa mã nguồn: Sử dụng các phương pháp tối ưu hóa mã nguồn, chẳng hạn như sử dụng minifier để giảm kích thước của mã HTML, CSS và JavaScript.
- Sử dụng các công cụ đo lường hiệu suất: Sử dụng các công cụ đo lường hiệu suất như Google PageSpeed Insights để theo dõi và đánh giá tốc độ tải trang web của bạn.

Tuy nhiên, việc tối ưu hóa tốc độ load trang là một quá trình liên tục và cần được thực hiện thường xuyên để đạt được hiệu quả tối đa.

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

1.4.1. Khái niệm và tính chất của dữ liệu khách hàng và đơn hàng

1.4.1.1. khái niệm dữ liệu khách hàng, đơn hàng

Dữ liệu khách hàng là thông tin về khách hàng mà doanh nghiệp thu thập được trong quá trình kinh doanh. Đây là tài nguyên quý giá giúp cho doanh nghiệp hiểu rõ hơn về thị trường và khách hàng của mình, từ đó có thể phát triển các chiến lược tiếp thị và bán hàng hiệu quả hơn.

Đơn hàng là một bản ghi chứa thông tin về sản phẩm hoặc dịch vụ mà khách hàng đã mua từ doanh nghiệp. Dữ liệu đơn hàng cho phép doanh nghiệp hiểu rõ

hơn về hành vi mua hàng của khách hàng, từ đó tối ưu hóa quá trình bán hàng và nâng cao chất lượng dịch vụ.

1.4.1.2. Tính chất dữ liệu khách hàng và đơn hàng

Dữ liệu khách hàng và đơn hàng là những dữ liệu quan trọng trong kinh doanh và tiếp thị hiện đại. Dữ liệu khách hàng bao gồm các thông tin về khách hàng như tên, địa chỉ email, số điện thoại, địa chỉ, lịch sử mua hàng, sở thích, quan tâm, v.v. Dữ liệu đơn hàng bao gồm các thông tin về sản phẩm hoặc dịch vụ được mua, giá, số lượng, phương thức thanh toán, ngày giao hàng, v.v.

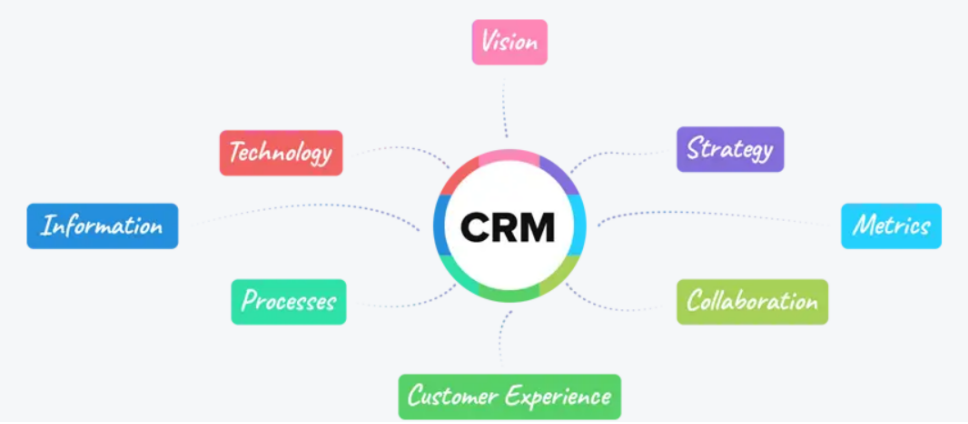
Tính chất của dữ liệu khách hàng và đơn hàng là:

- Có tính đa dạng: Dữ liệu khách hàng và đơn hàng có nhiều loại thông tin khác nhau như tên, địa chỉ, số điện thoại, lịch sử mua hàng, sở thích, quan tâm, v.v.
- Có tính trùng lặp: Một khách hàng có thể tạo ra nhiều đơn hàng, và một đơn hàng có thể chứa nhiều sản phẩm.
- Có tính thay đổi: Dữ liệu khách hàng và đơn hàng sẽ liên tục thay đổi theo thời gian khi khách hàng mua sản phẩm mới, đổi thông tin cá nhân hoặc hủy đơn hàng.
- Có tính cập nhật: Dữ liệu khách hàng và đơn hàng cần phải được cập nhật thường xuyên để đảm bảo tính chính xác và đầy đủ.
- Có tính ứng dụng cao: Dữ liệu khách hàng và đơn hàng được sử dụng để phân tích, định hướng chiến lược kinh doanh, làm nền tảng cho các chiến dịch tiếp thị và quản lý quan hệ khách hàng.

1.4.2. Các giải pháp quản lý dữ liệu hiệu quả

1.4.2.1. 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.



Hình 3: Tám khối xây dựng thiết yếu của nền tảng CRM

CRM là thị trường phần mềm lớn nhất trên thế giới và ngày càng được chứng minh là tài sản công nghệ tốt nhất mà các công ty có thể đầu tư. Với sự nổi bật mà thị trường phần mềm CRM nền tảng điện toán đám mây đã có được trong nhiều năm và việc CRM có thể dễ dàng tích hợp với nhiều ứng dụng khác mà các doanh nghiệp thường sử dụng, hệ thống CRM giúp người sử dụng bao quát mọi khía cạnh của chu kỳ kinh doanh, từ đó gia tăng doanh số và lợi nhuận tiếp thị, đồng thời cắt giảm chi phí.

Hình 4: Lợi ích của việc sử dụng hệ thống CRM

1.4.2.2. Hệ thống CRM có các loại

Một trong những sự lựa chọn đầu tiên mà doanh nghiệp phải đưa ra là lựa chọn hệ thống CRM tại chỗ hay CRM nền tảng đám mây. Với hệ thống CRM tại chỗ, doanh nghiệp thường phải thiết lập cơ sở hạ tầng phụ trợ hoàn chỉnh và chịu chi phí bảo trì và nâng cấp, ngoài phí giấy phép của phần mềm thực tế.

Hệ thống CRM nền tảng đám mây thường là lựa chọn được ưa thích nhất của nhiều doanh nghiệp vì hệ thống này có thể dễ dàng truy cập được qua bất kỳ trình duyệt nào, cho phép triển khai và sử dụng nhanh hơn. Các lợi ích phụ thêm khác

bao gồm không tốn chi phí bảo trì hoặc bảo dưỡng, khả năng truy cập dữ liệu tốt hơn khi cần và mở rộng hoặc thu gọn dễ dàng và linh hoạt.

1.4.2.3. Hệ thống CRM có các tính năng

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.

1.4.2.4. Quản lý đơn hàng

Trong quản lý đơn hàng, việc quản lý dữ liệu hiệu quả là rất quan trọng để giúp cho công việc của người quản lý được dễ dàng hơn và đảm bảo tính chính xác của thông tin. Dưới đây là một số giải pháp quản lý dữ liệu hiệu quả trong quản lý đơn hàng:

Sử dụng phần mềm quản lý đơn hàng: Phần mềm quản lý đơn hàng sẽ giúp bạn tổ chức và quản lý dữ liệu về sản phẩm, khách hàng, đơn hàng và các hoạt động khác liên quan đến quản lý đơn hàng. Nhờ đó, bạn sẽ có được cái nhìn toàn diện về tình trạng đơn hàng của mình và có thể đưa ra các quyết định kịp thời.

Xác định và sắp xếp các loại dữ liệu: Trong quản lý đơn hàng, các loại dữ liệu như thông tin khách hàng, thông tin sản phẩm, số lượng sản phẩm, giá sản phẩm, thông tin vận chuyển, thanh toán, v.v. nên được xác định và sắp xếp theo từng nhóm riêng biệt để dễ dàng quản lý và tra cứu.

Sử dụng mã định danh sản phẩm và khách hàng: Việc sử dụng mã định danh sản phẩm và khách hàng sẽ giúp bạn dễ dàng tìm kiếm thông tin và phân loại các đơn hàng, sản phẩm và khách hàng.

Quản lý cập nhật dữ liệu thường xuyên: Việc quản lý và cập nhật dữ liệu thường xuyên là rất quan trọng trong quản lý đơn hàng, giúp cho tình trạng dữ liệu

được cập nhật liên tục và chính xác, giảm thiểu việc nhập sai thông tin hoặc bị trùng lặp.

Thực hiện sao lưu dữ liệu thường xuyên: Để đảm bảo an toàn cho dữ liệu của mình, bạn nên thực hiện sao lưu dữ liệu thường xuyên để đối phó với các tình huống không mong muốn như mất dữ liệu do hỏng máy tính, virus, hay bị hacker tấn công.

Tóm lại, việc quản lý dữ liệu hiệu quả trong quản lý đơn hàng đóng vai trò quan trọng trong việc giúp cho công việc của người quản lý được dễ dàng hơn và đảm bảo tính chính xác của thông tin.

1.4.2.5. Quản lý kho hàng

Trong quản lý kho hàng, việc quản lý dữ liệu hiệu quả là rất quan trọng để giúp cho công việc của người quản lý được dễ dàng hơn và đảm bảo tính chính xác của thông tin. Dưới đây là một số giải pháp quản lý dữ liệu hiệu quả trong quản lý kho hàng:

Sử dụng phần mềm quản lý kho hàng: Phần mềm quản lý kho hàng sẽ giúp bạn tổ chức và quản lý dữ liệu về sản phẩm, số lượng sản phẩm, đơn vị đo lường, vị trí trong kho, v.v. Nhờ đó, bạn sẽ có được cái nhìn toàn diện về tình trạng kho hàng của mình và có thể đưa ra các quyết định kịp thời.

Xác định và sắp xếp các loại dữ liệu: Trong quản lý kho hàng, các loại dữ liệu như thông tin sản phẩm, số lượng sản phẩm, đơn vị đo lường, vị trí trong kho, v.v. nên được xác định và sắp xếp theo từng nhóm riêng biệt để dễ dàng quản lý và tra cứu.

Sử dụng mã định danh sản phẩm và vị trí trong kho: Việc sử dụng mã định danh sản phẩm và vị trí trong kho sẽ giúp bạn dễ dàng tìm kiếm thông tin và phân loại các sản phẩm, đồng thời quản lý được việc xuất nhập kho.

Quản lý cập nhật dữ liệu thường xuyên: Việc quản lý và cập nhật dữ liệu thường xuyên là rất quan trọng trong quản lý kho hàng, giúp cho tình trạng dữ liệu được cập nhật liên tục và chính xác, giảm thiểu việc nhập sai thông tin hoặc bị trùng lặp.

Thực hiện sao lưu dữ liệu thường xuyên: Để đảm bảo an toàn cho dữ liệu của mình, bạn nên thực hiện sao lưu dữ liệu thường xuyên để đối phó với các tình huống không mong muốn như mất dữ liệu do hỏng máy tính, virus, hay bị hacker tấn công.

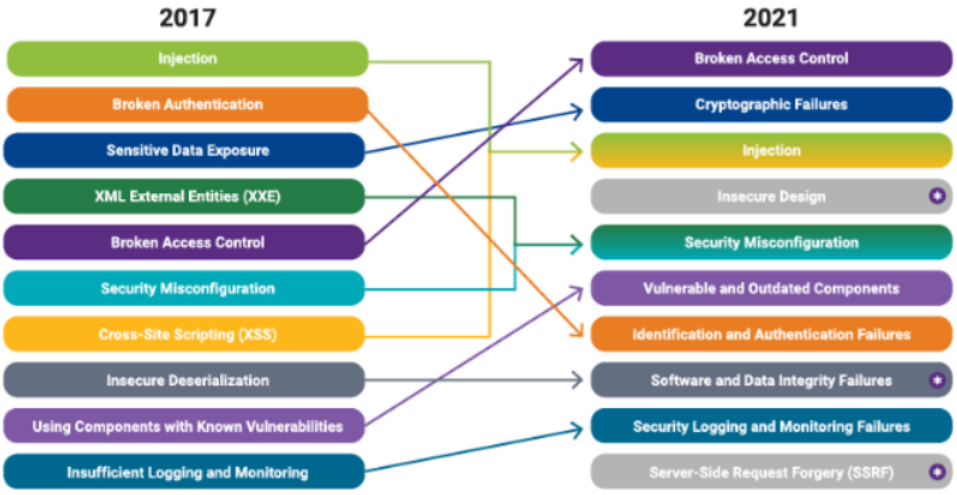
Tóm lại, việc quản lý dữ liệu hiệu quả trong quản lý kho hàng đóng vai trò quan trọng trong việc giúp cho công việc của người quản lý được dễ dàng hơn và đảm bảo tính chính xác của thông tin.

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

Top 10 lỗ hổng OWASP là danh sách các lỗ hổng bảo mật phổ biến nhất trong ứng dụng web. Nó được phát triển bởi OWASP (Open Web Application Security Project) và tập trung vào việc cải thiện bảo mật cho các ứng dụng web.

OWASP (Open Web Application Security Project) là một tổ chức phi lợi nhuận được thành lập với mục đích tập trung vào việc cải thiện bảo mật cho các ứng dụng web. Tổ chức này liên tục đón nhận đóng góp từ các chuyên gia an ninh mạng, hacker mũ trắng, các sàn Bug Bounty và các tổ chức bảo mật trên toàn thế giới về các lỗ hổng bảo mật và các kỹ thuật tấn công mới nhất.

Danh sách Top 10 lỗ hổng OWASP bao gồm các lỗ hổng bảo mật nguy hiểm nhất mà các nhà phát triển ứng dụng web cần phải biết để có thể bảo vệ ứng dụng web của họ khỏi các cuộc tấn công từ tin tặc và các mối đe dọa bảo mật khác.



Hình 5: Danh sách lỗ hổng Top 10 OWASP 2023

Cứ 3 năm một lần, danh sách này được cập nhật và sửa đổi để phù hợp với các lỗ hổng bảo mật mới nhất và các kỹ thuật tấn công mới nhất. Nắm vững danh sách Top 10 lỗ hổng OWASP sẽ giúp các nhà phát triển ứng dụng web có thể bảo vệ ứng dụng của họ khỏi các mối đe dọa bảo mật đáng lo ngại nhất.

Dưới đây là danh sách Top 10 lỗ hổng OWASP được cập nhật mới nhất vào năm 2021: [1]

- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design (Lỗ hổng mới cập nhật)
- Security Misconfiguration
- Vulnerable and Outdated Components

- Identification and Authentication Failures
- Software and Data Integrity Failures (Lỗ hổng mới cập nhật)
- Security Logging and Monitoring Failures
- Server-Side Request Forgery (SSRF) (Lỗ hổng mới cập nhật)

Giải pháp để khắc phục các lỗ hổng Top 10 OWASP

Để khắc phục các lỗ hổng bảo mật liên quan đến danh sách Top 10 OWASP, các nhà phát triển ứng dụng web có thể áp dụng các giải pháp sau:

- Thực hiện kiểm tra bảo mật (Web Penetration Testing) và phát hiện các lỗ hổng tiềm ẩn trước khi ứng dụng được triển khai.
- Sử dụng các giải pháp bảo mật đáng tin cậy để ngăn chặn các cuộc tấn công trên các lỗ hổng bảo mật phổ biến nhất.
- Thực hiện Pentest thường xuyên và cập nhật các bản vá lỗ hổng bảo mật mới nhất cho các thư viện, framework, module của ứng dụng web.
- Đào tạo nhân viên về các vấn đề bảo mật và hãy đảm bảo rằng họ phải có các kiến thức và kỹ năng lập trình an toàn cần thiết để bảo vệ ứng dụng.

1.5.1. Broken Access Control (phá vỡ kiểm soát truy cập)

Kiểm soát truy cập là sự kiểm soát người dùng không cho phép họ thực thi những hành động bên ngoài quyền hạn. Các lỗi thường dẫn đến tiết lộ thông tin trái phép, sửa đổi hoặc phá hủy tất cả dữ liệu hoặc thực hiện chức năng ngoài giới hạn của người dùng.

Các lỗ hổng phổ biến

- Sửa đổi URL
- Sửa đổi thông tin nhận dạng để truy cập tài khoản người khác (IDOR)
- Leo thang đặc quyền

Cách ngăn chặn

- Ngoại trừ tài nguyên công cộng, còn lại từ chối theo mặc định
- Xác thực người dùng khi học quay lại ứng dụng
- Kiểm tra quyền tại thời điểm người dùng cố gắng thực hiện hành động

Ví dụ: Kẻ tấn công chỉ cần buộc các trình duyệt đến các URL mục tiêu. Quyền quản trị được yêu cầu để truy cập vào trang quản trị https://example.com/app/getappInfo, https://example.com/app/admin

1.5.2. Cryptographic Failures (lỗi mật mã bị hỏng)

Bảo mật thông tin nhạy cảm bằng cách mã hóa thông tin theo các cách khác nhau, nhưng nếu cách mã hóa đó kẻ tấn công có thể giải mã được hay là cách thức

giải mã không đảm bảo an toàn bản rõ thì những thông tin nhạy cảm đó sẽ bị rò rỉ ra ngoài.

Các lỗi phổ biến

- Sử dụng những giao thức truyền dữ liệu dạng rõ như HTTP, FTP,…
- Sử dụng những mã hóa đã cũ hoặc yếu
- Sử dụng những hàm băm không dùng nữa như md5, SHA1
- Khóa bí mật dễ đoán
- Chuỗi mã hóa không được xác thực

Cách ngăn chặn

- Không sử dụng những giao thức đã cũ như FTP, SMTP,… để vận chuyển dữ liệu nhạy cảm
- Đảm bảo các thuật toán mã hóa đạt tiêu chuẩn mạnh mẽ
- Mã hóa dữ liệu trên đường truyền bằng TLS, HTTPS
- Lưu trữ password bằng các hàm băm mạnh như Argon2, scrypt, bcrypt,…
- Luôn sử dụng mã hóa được xác thực thay vì chỉ mã hóa

Ví dụ: Một trang web không sử dụng TLS cho tất cả các trang hoặc hỗ trợ mã hóa yếu. Kẻ tấn công giám sát lưu lượng mạng (như tại một mạng không dây không an toàn), hạ cấp các kết nối từ HTTPS xuống HTTP, chặn các yêu cầu và đánh cắp cookie phiên của người dùng. Sau đó, kẻ tấn công phát lại cookie này và chiếm quyền điều khiển phiên của người dùng, truy cập hoặc sửa đổi dữ liệu cá nhân của người dùng. Thay vì những điều trên, họ có thể thay đổi tất cả dữ liệu được vận chuyển, ví dụ như người nhận chuyển tiền.

1.5.3. 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.

1.5.4. Insecure Design (Thiết kế không an toàn)

Thiết kế an toàn là phân tích các giả định và điều kiện cho các dòng dự kiến đảm bảo chính xác, tránh trường hợp không mong muốn và có hành vi phù hợp với từng trường hợp. Đảm bảo kết quả được ghi lại trong nhật kí của người dùng. Học hỏi từ những sai lầm và đưa ra những cải tiến thích hợp. Cách ngăn chặn

- Thiết lập sử dụng những thư viện mẫu thiết kế an toàn
- Kiểm tra tính hợp lí ở mỗi cấp ứng dụng
- Tách các lớp phần trên hệ thống và các lớp mạng
- Hạn chế tiêu thụ tài nguyên người dùng hoặc dịch vụ

Ví dụ: Một rạp chiếu phim cho phép đặt chỗ theo nhóm tối đa 15 người trước khi đặt tiền cọc, một kẻ tấn công có thể chạy lệnh để đặt tất cả các chỗ trong rạp sau đó dừng lại ở bước đặt cọc, gây tổn thất lớn về kinh tế

1.5.5. Security Misconfiguration (Cấu hình bảo mật sai)

Nếu Insecure Design thuộc về phần thiết kế thì Security Misconfiguration thuộc về phần triển khai. Những lỗi phổ biến thường xảy ra

- Các tính năng không cần thiết được bật như các port, service, account,…
- Thiếu việc tăng cường bảo mật cho từng phần của ứng dụng
- Các tài khoản và mật khẩu vẫn để mặc định không thay đổi
- Phần mềm đã lỗi thời

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
- Loại bỏ những tài nguyên, tính năng không cần thiết
- Cung cấp sự hiệu quả và an toàn giữa các thành phần
- Liên tục cập nhật những phiên bản mới nhất

Ví dụ: Danh sách thư mục không bị tắt trên máy chủ. Kẻ tấn công phát hiện ra chúng có thể liệt kê các thư mục một cách đơn giản. Điều này có thể dẫn đến kẻ tấn công dịch ngược lại đoạn code và là tiềm ẩn rất lớn cho nhiều mối nguy hiểm khác

1.5.6. Các thành phần dễ bị tổn thương và lỗi thời

Những lỗi phổ biến
- Không quét lỗ hổng thường xuyên và đăng ký nhận các bản tin bảo mật liên quan đến các thành phần bạn sử dụng
- Phần mềm dễ bị tấn công: không được hỗ trợ hoặc lỗi thời
- Không sửa chữa, nâng cấp các nền tảng
- Không bảo mật cấu hình của các thành phần

Cách ngăn chặn
- Loại bỏ các phụ thuộc không sử dụng, các tính năng, thành phần, tệp và tài liệu không cần thiết
- Liên tục kiểm tra các phiên bản của cả thành phần phía máy khách và máy chủ
- Chính lấy các thành phần từ nguồn chính thức qua các liên kết an toàn

Ví dụ: Các thành phần thường chạy với các đặc quyền giống như chính ứng dụng đó, vì vậy sai sót trong bất kỳ thành phần nào có thể dẫn đến tác động nghiêm trọng. Những sai sót như vậy có thể là ngẫu nhiên hoặc cố ý.

1.5.7. Nhận dạng và xác thực bị hỏng

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:

- Sử dụng xác thực đa yếu tố một cách an toàn
- Giới hạn số lần xác thực nhất định
- Thực hiện kiểm tra mật khẩu yếu và yêu cầu mật khẩu có độ phức tạp nhất định
- Đảm bảo các đường dẫn khôi phục thông tin xác thực và API được tăng cường chống lại các cuộc tấn công
- Sử dụng trình quản lí phiên tích hợp an toàn, tạo ID ngẫu nhiên mới với độ phức tạp cao

Ví dụ: Bạn đặt mật khẩu quá dễ đoán hay là ứng dụng không giới hạn số lần đăng nhập và kẻ tấn công thực hiện cuộc tấn công từ điển

1.5.8. Lỗi toàn vẹn dữ liệu và phần mềm

Các lỗi về tính toàn vẹn của phần mềm và dữ liệu liên quan đến code và cơ sở hạ tầng không bảo vệ khỏi các vi phạm tính toàn vẹn:

- Ứng dụng dựa vào các plugin, thư viện hoặc mô-đun không đáng tin cậy, không an toàn. Dẫn đến truy cập trái phép, thực thi các mã độc hại hoặc xâm nhập hệ thống
- Tự động cập nhật các bản cập nhật mà không xác minh tính toàn vẹn đầy đủ và được áp dụng cho phiên bản trước đó

Cách ngăn chặn:

- Sử dụng chữ kí số để xác minh phần mềm
- Đảm bảo các thư viện và phần phụ thuộc
- Có công cụ bảo mật để kiểm tra độ an toàn phần mềm
- Đảm bảo những dữ liệu chưa được kí hoặc chưa được mã hóa không gửi đến các máy khách không đáng tin cậy

Ví dụ: Cập nhật mà không cần kí, người dùng sẽ vô tình tải về những bản cập nhật chứa mã độc mà kẻ tấn công cố tình phát tán trên mạng để đánh cắp thông tin hay khai thác dữ liệu trong máy nạn nhân

1.5.9. Các lỗi theo dõi và ghi nhật kí bảo mật

Ghi nhật kí bảo mật nhằm giúp phát hiện, báo cáo và phản hồi các vi phạm nhằm kịp thời ngăn chặn các cuộc tấn công nguy hiểm. Ghi nhật kí giám sát và phản hồi không đầy đủ có thể xảy ra bất cứ lúc nào

- Các sự kiện quan trọng như đăng nhập không thành công hay những thao tác có tác động lớn không được ghi lại
- Các cảnh báo lỗi không thông báo, không đầy đủ hoặc không rõ ràng
- Nhật kí các hoạt động API không được giám sát
- Ứng dụng không thể hoặc phản hồi quá chậm các phát hiện, báo cáo hoặc cảnh báo về các cuộc tấn công đang hoạt động trong thời gian thực

Cách ngăn chặn

- Đảm bảo các lỗi đăng nhập, kiểm soát truy cập và xác thực đầu vào phía máy chủ được ghi lại đủ để xác định các tài khoản đáng ngờ
- Đảm bảo nhật kí được mã hóa chính xác tránh việc tiêm hoặc tấn công vào hệ thống ghi nhật kí hoặc giám sát
- Đảm bảo các hành động tác động lớn được kiểm tra với các biện pháp kiểm soát tính toàn vẹn để ngăn chặn việc giả mạo hoặc xóa, chẳng hạn như bảng cơ sở dữ liệu chỉ được thêm vào

- Các nhóm DevSecOps nên thiết lập giám sát và cảnh báo hiệu quả để các hoạt động đáng ngờ được phát hiện và phản hồi nhanh chóng

Ví dụ: Một hãng hàng không lớn của Ấn Độ đã bị vi phạm dữ liệu liên quan đến dữ liệu cá nhân của hàng triệu hành khách trong hơn mười năm, bao gồm cả dữ liệu hộ chiếu và thẻ tín dụng. Vi phạm dữ liệu xảy ra tại một nhà cung cấp dịch vụ lưu trữ đám mây bên thứ ba, người này đã thông báo cho hãng hàng không về vi phạm sau một thời gian

1.5.10. Giả mạo yêu cầu phía máy chủ

SSRF xảy ra bất cứ khi nào khi ứng dụng web đang tìm nạp tài nguyên từ xa mà không xác thực URL do người dùng cung cấp. Nó cho phép kẻ tấn công ép ứng dụng gửi một yêu cầu đến một điểm đích không mong muốn, ngay cả khi được bảo vệ bởi tường lửa Cách ngăn chặn Lớp mạng

- Phân đoạn chức năng truy cập tài nguyên từ xa trong các mạng riêng biệt để giảm tác động của SSRF
- Thực thi các chính sách tường lửa "từ chối theo mặc định" hoặc các quy tắc kiểm soát truy cập mạng để chặn tất cả trừ lưu lượng mạng nội bộ thiết yếu

Lớp ứng dụng

- Làm sạch và xác thực tất cả dữ liệu đầu vào do người dùng cung cấp
- Thực thi lược đồ URL, cổng là điểm đến với danh sách cho phép xác thực
- Tắt chuyển hướng HTTP

Ví dụ: Những kẻ tấn công có thể truy cập các tệp cục bộ chẳng hạn như hoặc các dịch vụ nội bộ để lấy thông tin nhạy cảm như file:

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

1.6.1. SSL - Secure Socket Layer

SSL (Secure Socket Layer) là một công nghệ mã hóa dữ liệu được sử dụng để bảo vệ thông tin truyền tải giữa các máy tính trên mạng Internet. SSL giúp đảm bảo rằng thông tin được truyền từ người dùng đến máy chủ và ngược lại là an toàn và không thể bị đánh cắp hoặc chỉnh sửa trong quá trình truyền.

Khi bạn kết nối đến một trang web an toàn, giao thức HTTPS được sử dụng, điều này có nghĩa là trang web đã được bảo vệ bởi SSL. Khi bạn truy cập trang web này, trình duyệt của bạn sẽ thiết lập một kết nối an toàn với máy chủ thông qua SSL. Trong quá trình này, thông tin được truyền giữa trình duyệt và máy chủ được mã hóa để đảm bảo tính bảo mật.

SSL sử dụng một phương thức mã hóa gọi là mã hóa khóa công khai (public key encryption) để bảo vệ thông tin truyền tải. Điều này có nghĩa là thông tin được mã hóa bởi một khóa công khai được cung cấp bởi máy chủ, và chỉ có thể được giải mã bằng khóa riêng tư được giữ bí mật trên máy chủ. Khi thông tin được gửi từ trình duyệt của người dùng đến máy chủ, nó sẽ được mã hóa bằng khóa công khai và chỉ có thể được giải mã bởi máy chủ với khóa riêng tư tương ứng.

SSL là một trong những công nghệ bảo mật trực tuyến quan trọng nhất và được sử dụng rộng rãi trong các ứng dụng web, email và các ứng dụng trực tuyến khác.

1.6.2. Tokenization

Mã hóa không phải là cách duy nhất để che giấu giá trị số nhận dạng tài chính hoặc thông tin cá nhân của người dùng. Tokenization là một quá trình mà trong đó thông tin thanh toán nhạy cảm của người sử dụng được thay thế bằng một tập hợp các ký tự được gọi là token và các token này sẽ không ảnh hưởng đến tính an toàn trong các giao dịch trực tuyến và di động. Các máy khách sẽ thực hiện truyền mã token, thay vì dữ liệu thông tin gốc quan trọng, điều này khiến dữ liệu sẽ không thể bị đánh cắp hoặc không có giá trị đối với kẻ tấn công khi đánh cắp được.

Không giống với chức năng của hệ thống mã hóa, hệ thống sử dụng phương thức tokenization sẽ thực hiện tạo ra token mới cho mỗi người dùng mới, liên kết dữ liệu gốc với token nhưng không thực hiện giải mã token và làm lộ dữ liệu gốc.

Ví dụ, tại một sòng bạc, những người chơi đánh bạc sẽ nhận được các token để đổi lấy một số lượng tiền mặt. Sòng bạc sẽ cho phép người chơi đánh bạc bằng các token này mà không cần sử dụng tiền mặt thực tế. Nếu token bị đánh cắp thì những token đó sẽ không thể được sử dụng trong các sòng bạc khác.

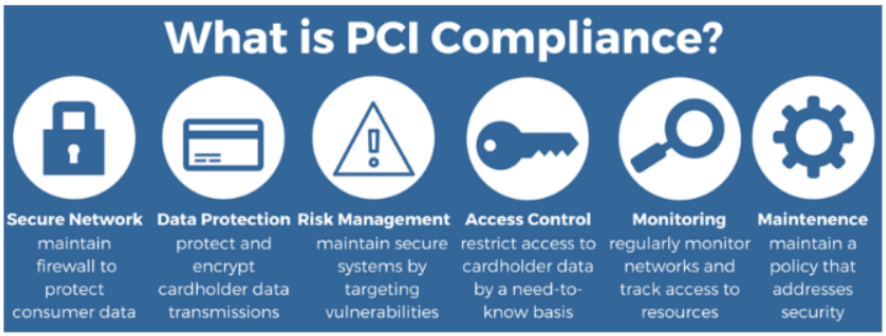
1.6.3. 3D Secure

3D Secure là một phương thức xác thực thanh toán trực tuyến được sử dụng bởi các ngân hàng và tổ chức thẻ tín dụng để cung cấp cho khách hàng một lớp bảo vệ bổ sung khi sử dụng thẻ của họ để mua hàng trực tuyến. Khi giao dịch được khởi tạo, khách hàng sẽ được yêu cầu cung cấp thông tin xác thực bổ sung, chẳng hạn như mật khẩu hoặc mã OTP (One-Time Password), trước khi giao dịch được phê duyệt. Điều này giúp đảm bảo rằng chỉ có chủ sở hữu của thẻ mới có thể thực hiện giao dịch và giảm thiểu rủi ro gian lận trong các giao dịch trực tuyến. 3D Secure là một phương thức xác thực thanh toán trực tuyến được sử dụng để bảo vệ các giao dịch trực tuyến khỏi các hoạt động gian lận. Phương thức này yêu cầu khách hàng cung cấp thông tin xác thực bổ sung như mật khẩu hoặc mã OTP trước khi giao dịch được phê duyệt.

Khi khách hàng thực hiện giao dịch trực tuyến, nếu ngân hàng hoặc tổ chức thẻ của họ hỗ trợ 3D Secure, họ sẽ được chuyển tiếp đến trang xác thực riêng của ngân hàng hoặc tổ chức thẻ. Trang web này sẽ yêu cầu khách hàng cung cấp thông tin xác thực bổ sung, chẳng hạn như mật khẩu hoặc mã OTP, để xác minh danh tính của họ. Sau khi thông tin được cung cấp và xác thực thành công, giao dịch sẽ được phê duyệt và tiền sẽ được chuyển vào tài khoản người bán hàng.

Với 3D Secure, khách hàng có thể yên tâm khi thực hiện giao dịch trực tuyến vì phương thức này giúp hạn chế rủi ro bị gian lận và tránh bị mất tiền của mình.

1.6.4. PCI DSS Compliance- Tuân thủ Tiêu chuẩn An ninh Dữ liệu Thẻ



Hình 6: OWASP Top 10 2023

PCI DSS viết tắt cho Payment Card Industry Data Security Standard là một tiêu chuẩn an ninh thông tin bắt buộc dành cho các doanh nghiệp lưu trữ, truyền tải và xử lý thẻ thanh toán quản lý bởi 05 tổ chức thanh toán quốc tế như Visa, MasterCard, American Express, Discover và JCB. PCI DSS là một tiêu chuẩn được các tổ chức thanh toán quốc tế nêu trên ủy quyền quản lý cho Hội đồng Bảo mật dữ liệu thẻ thanh toán PCI SSC (Payment Card Industry Security Standard Council). PCI DSS (Payment Card Industry Data Security Standard) là một tiêu chuẩn an ninh thông tin của ngành thanh toán thẻ. Tiêu chuẩn này được thiết kế nhằm bảo vệ thông tin dữ liệu thẻ tín dụng và ngăn chặn các cuộc tấn công trên hệ thống thanh toán.

Để đạt được tuân thủ PCI DSS, các doanh nghiệp phải thực hiện theo một loạt các yêu cầu khắt khe, chẳng hạn như:

Thực hiện bảo mật hệ thống và mạng để bảo vệ dữ liệu thẻ tín dụng.

Bảo vệ các thông tin xác thực của khách hàng bằng cách sử dụng các giải pháp mã hóa.

Thực hiện quản lý quy trình và chính sách bảo mật, đảm bảo rằng nhân viên được đào tạo và thực hiện theo tiêu chuẩn an ninh thông tin.

Quản lý rủi ro và đánh giá các điểm yếu trong hệ thống để đảm bảo rằng các bước bảo vệ được triển khai một cách hiệu quả.

Đảm bảo rằng các bên liên quan, chẳng hạn như nhà cung cấp dịch vụ thanh toán và đối tác kinh doanh, cũng tuân thủ các yêu cầu của PCI DSS.

Việc tuân thủ PCI DSS là rất quan trọng để bảo vệ thông tin cá nhân và tài khoản ngân hàng của khách hàng. Các doanh nghiệp có thể áp dụng các giải pháp công nghệ để đảm bảo tiêu chuẩn an ninh này, hoặc thuê các nhà cung cấp dịch vụ chuyên nghiệp để hỗ trợ cho việc tuân thủ PCI DSS.

1.6.5. OAuth

OAuth (Open Authorization) là một giao thức xác thực và ủy quyền được sử dụng để cho phép người dùng cấp quyền truy cập tài khoản của mình cho các ứng dụng, dịch vụ và trang web khác.

OAuth cho phép người dùng chia sẻ thông tin cá nhân và tài khoản của họ mà không cần tiết lộ mật khẩu của mình. Thay vào đó, OAuth sử dụng một mã truy cập để cung cấp quyền truy cập. Khi người dùng cấp quyền truy cập cho ứng dụng, dịch vụ hoặc trang web, mã truy cập sẽ được tạo ra. Mã này sau đó được sử dụng để xác thực yêu cầu truy cập từ ứng dụng, dịch vụ hoặc trang web đó.

Ví dụ, nếu bạn muốn sử dụng tài khoản Facebook của mình để đăng nhập vào một ứng dụng khác, thì ứng dụng đó sẽ yêu cầu bạn cấp quyền truy cập vào tài khoản Facebook của mình. Nếu bạn đồng ý, mã truy cập sẽ được tạo ra và ứng dụng sẽ sử dụng nó để yêu cầu các thông tin từ tài khoản Facebook của bạn. Bằng cách này, bạn không cần phải tiết lộ mật khẩu của mình cho ứng dụng khác.

OAuth là một giao thức quan trọng trong việc xác thực và ủy quyền truy cập dữ liệu trên Internet. Nó được sử dụng rộng rãi trong các ứng dụng web và di động để giúp người dùng dễ dàng chia sẻ thông tin của họ và tạo ra trải nghiệm người dùng thuận tiện hơn.

1.6.6. Secure Payment Protocols

Secure Payment Protocol (SPP) là một giao thức thanh toán trực tuyến được thiết kế để đảm bảo rằng các giao dịch thanh toán được thực hiện một cách an toàn và bảo mật. Giao thức này được xây dựng trên cơ sở các tiêu chuẩn bảo mật hàng đầu hiện nay và đảm bảo rằng thông tin thanh toán được mã hóa và bảo mật trong suốt quá trình truyền tải. SPP sử dụng các phương pháp mã hóa và xác thực để đảm bảo tính toàn vẹn của dữ liệu trong quá trình truyền tải. SPP cũng được thiết kế để

hỗ trợ các hình thức thanh toán trực tuyến khác nhau, bao gồm thẻ tín dụng, thẻ ghi nợ và tài khoản ngân hàng trực tuyến.

Secure Payment Protocols (giao thức thanh toán an toàn) là các chuỗi quy trình được thiết kế để đảm bảo tính toàn vẹn, bảo mật và sự riêng tư của thông tin liên quan đến các giao dịch thanh toán. Mục đích của các giao thức thanh toán an toàn là đảm bảo rằng các giao dịch thanh toán được thực hiện một cách an toàn, tin cậy và bảo mật.

Các giao thức thanh toán an toàn có thể bao gồm các quy trình như xác thực người dùng, mã hóa dữ liệu, xác thực ngân hàng hoặc tổ chức thanh toán, xác thực thẻ thanh toán, xác thực các giao dịch và giám sát giao dịch để phát hiện các hoạt động gian lận.

Một trong những yếu tố quan trọng trong các giao thức thanh toán an toàn là tính khả thi. Các giao thức thanh toán an toàn phải có khả năng thực hiện trên nhiều nền tảng và thiết bị khác nhau để đảm bảo rằng các giao dịch thanh toán có thể được thực hiện dễ dàng và tiện lợi. Các giao thức thanh toán an toàn cũng phải đảm bảo tính toàn vẹn của thông tin. Điều này có nghĩa là thông tin được truyền đi và lưu trữ trong quá trình thanh toán phải được bảo vệ và không thể bị thay đổi hoặc tấn công từ bên ngoài.

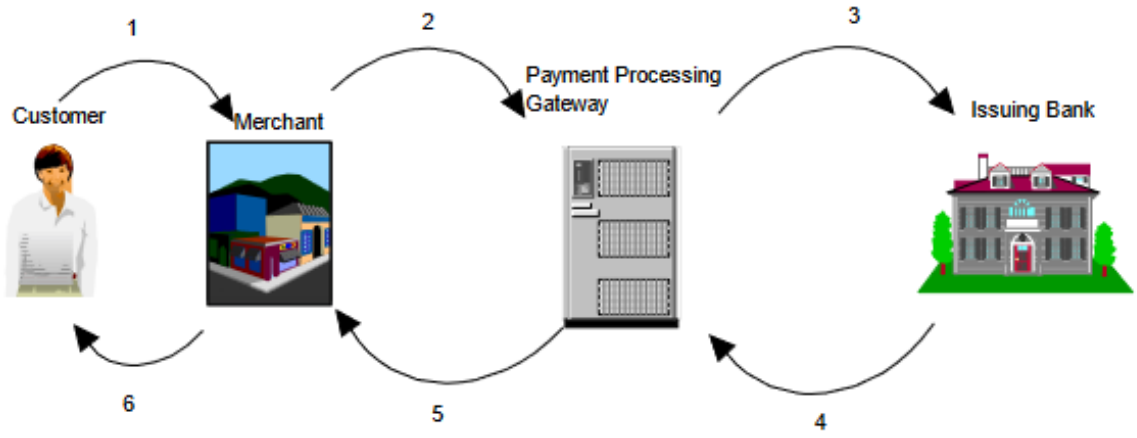
Ngoài ra, các giao thức thanh toán an toàn còn phải đảm bảo sự riêng tư của thông tin. Điều này có nghĩa là thông tin thanh toán không được chia sẻ với bất kỳ bên thứ ba nào, trừ khi được sự cho phép của người dùng.

1.7. Giao thức Secure Payment Protocol

1.7.1. Tổng quan Secure Payment Protocol

1.7.1.1. Tổng quan về xử lý thanh toán điện tử

Xử lý thanh toán trên internet tương tự như các phương pháp truyền thống để xử lý thanh toán bằng thẻ tín dụng. Trên internet, cửa hàng và giao dịch đều là ảo, có nghĩa là thẻ không được cà trực tiếp bằng máy. Người bán không thể nhìn thấy thẻ và xác minh tên của khách hàng hoặc chữ ký trên thẻ. Trong một giao dịch như vậy, người bán chịu trách nhiệm cho các giao dịch gian lận bởi các công ty thẻ tín dụng. Thế nên việc xử lý thanh toán trên internet người bán phải thực hiện các bước bảo vệ khác nhau chống lại gian lận trực tuyến, chẳng hạn như xác minh thông tin thẻ tín dụng được gửi bởi chính chủ sở hữu thẻ và bảo vệ cửa hàng trực tuyến và hạ tầng mạng của họ chống lại hacker.



Hình 7: Giao dịch thanh toán trên internet

Quá trình xác nhận thanh toán trực tuyến điển hình được thực hiện như sau:

- Bước 1: Khách hàng quyết định mua hàng trên trang web của người bán và tiếp tục thanh toán bằng cách cung cấp thông tin thẻ tín dụng của mình.
- Bước 2: Trang web của người bán nhận thông tin đơn hàng và thanh toán của khách hàng và gửi thông tin giao dịch thanh toán đến cổng xử lý thanh toán.
- Bước 3: Cổng xử lý thanh toán gửi thông tin thanh toán đến ngân hàng.
- Bước 4: Ngân hàng phát hành xác minh thông tin thanh toán và gửi kết quả, có thể là một số xác nhận hoặc từ chối thanh toán, đến cổng xử lý thanh toán, người sau đó chuyển kết quả đến người bán ở bước.
- Bước 5: Độ phức tạp của thuật toán xác nhận phụ thuộc vào giao thức thanh toán được sử dụng. Một dạng đơn giản của việc xác nhận sẽ đảm bảo rằng địa chỉ thanh toán được cung cấp bởi khách hàng cùng với thông tin thẻ tín dụng phù hợp với dữ liệu ở phía ngân hàng. Một số phương pháp mật mã xác nhận phức tạp hơn sẽ sử dụng để chứng thực chẳng hạn như chứng chỉ số, chữ ký số và bản rút trích số để xác minh rằng khách hàng là chủ sở hữu hợp pháp của thẻ tín dụng.
- Bước 6: người bán chấp nhận hoặc từ chối giao dịch và vận chuyển hàng hóa nếu cần thiết.

1.7.1.2. Giới thiệu và định nghĩa Secure Payment Protocol

Trong thời đại của cuộc cách mạng công nghiệp 4.0, các phương tiện thanh toán điện tử ngày càng trở nên phổ biến hơn. Với sự phát triển của thương mại điện tử, nhu cầu bảo mật và đảm bảo tính toàn vẹn dữ liệu trong quá trình thanh toán trực tuyến càng trở nên quan trọng hơn bao giờ hết. Để giải quyết vấn đề này, các giao thức thanh toán được phát triển và giới thiệu. Một số giao thức thanh toán an toàn hiện nay đã được giới thiệu và áp dụng rộng rãi trong như là SET (Secure Electronic Transaction), Cybercash, PCI DSS, 3D Secure thường được dùng cho thanh toán

trực tuyến và thường dùng kết hợp với SSL (Secure Sockets Layer) và TLS (Transport Layer Security). Những thứ đó được gọi chung là Secure Payment Protocols (SPP).

SPP là một tiêu chuẩn thanh toán trực tuyến được thiết kế để đảm bảo rằng các giao dịch thanh toán được thực hiện một cách an toàn và bảo mật. Giao thức này được xây dựng trên cơ sở các tiêu chuẩn bảo mật hàng đầu hiện nay và đảm bảo rằng thông tin thanh toán được mã hóa và bảo mật trong suốt quá trình truyền tải. SPP sử dụng các phương pháp mã hóa và xác thực để đảm bảo tính toàn vẹn của dữ liệu trong quá trình truyền tải. SPP cũng được thiết kế để hỗ trợ các hình thức thanh toán trực tuyến khác nhau, bao gồm thẻ tín dụng, thẻ ghi nợ và tài khoản ngân hàng trực tuyến.

SPP là các chuỗi quy trình được thiết kế để đảm bảo tính toàn vẹn, bảo mật và sự riêng tư của thông tin liên quan đến các giao dịch thanh toán. Mục đích của các giao thức thanh toán an toàn là đảm bảo rằng các giao dịch thanh toán được thực hiện một cách an toàn, tin cậy và bảo mật.

Các giao thức thanh toán an toàn có thể bao gồm các quy trình như xác thực người dùng, mã hóa dữ liệu, xác thực ngân hàng hoặc tổ chức thanh toán, xác thực thẻ thanh toán, xác thực các giao dịch và giám sát giao dịch để phát hiện các hoạt động gian lận.

Một trong những yếu tố quan trọng trong các giao thức thanh toán an toàn là tính khả thi. Các giao thức thanh toán an toàn phải có khả năng thực hiện trên nhiều nền tảng và thiết bị khác nhau để đảm bảo rằng các giao dịch thanh toán có thể được thực hiện dễ dàng và tiện lợi.

Các giao thức thanh toán an toàn cũng phải đảm bảo tính toàn vẹn của thông tin. Điều này có nghĩa là thông tin được truyền đi và lưu trữ trong quá trình thanh toán phải được bảo vệ và không thể bị thay đổi hoặc tấn công từ bên ngoài. Ngoài ra, các giao thức thanh toán an toàn còn phải đảm bảo sự riêng tư của thông tin. Điều này có nghĩa là thông tin thanh toán không được chia sẻ với bất kỳ bên thứ ba nào, trừ khi được sự cho phép của người dùng.

1.7.1.3. Các tiêu chuẩn thiết kế SPP

Tiêu chuẩn thiết kế Secure Payment Protocols bao gồm các yếu tố cơ bản sau:

- Bảo mật dữ liệu: Hệ thống thanh toán trực tuyến cần đảm bảo tính bảo mật của dữ liệu giao dịch. Điều này có thể được đảm bảo bằng cách sử dụng mã hóa dữ liệu, cơ chế xác thực, các phương pháp bảo vệ chống lại tấn công mạng và các cơ chế quản lý danh tính.

- Tính sẵn sàng và tin cậy: Hệ thống thanh toán trực tuyến phải được thiết kế để có khả năng hoạt động liên tục, đảm bảo tính sẵn sàng cao. Đồng thời, hệ thống cần đảm bảo tính tin cậy cao, giảm thiểu thời gian ngưng trệ hoặc lỗi hệ thống.
- Khả năng mở rộng: Hệ thống thanh toán trực tuyến cần có khả năng mở rộng, đáp ứng được nhu cầu mở rộng của doanh nghiệp trong tương lai, có thể được tích hợp với các dịch vụ mới và phát triển các tính năng mới.
- Thân thiện với người dùng: Giao diện và trải nghiệm người dùng của hệ thống thanh toán trực tuyến cần được thiết kế đơn giản, dễ sử dụng, giúp người dùng dễ dàng tiến hành các giao dịch thanh toán.
- Tuân thủ các quy định và tiêu chuẩn bảo mật: Hệ thống thanh toán trực tuyến cần tuân thủ các quy định và tiêu chuẩn bảo mật, chẳng hạn như PCI DSS, ISO 27001, GDPR và các quy định của cơ quan quản lý nhà nước.
- Hỗ trợ đa nền tảng: Hệ thống thanh toán trực tuyến cần hỗ trợ đa nền tảng, đảm bảo tính tương thích và khả năng tích hợp với các nền tảng khác nhau.

Các yếu tố trên đây là những yếu tố quan trọng trong việc thiết kế một hệ thống thanh toán trực tuyến an toàn và bảo mật. Ngoài ra, các nhà thiết kế cần liên tục cập nhật và nghiên cứu các công nghệ mới, các phương pháp bảo mật mới để cải thiện tính an toàn và bảo mật của hệ thống thanh toán trực tuyến. Việc đảm bảo an toàn và bảo mật cho người dùng là rất quan trọng trong ngành công nghiệp thanh toán trực tuyến và sẽ tạo niềm tin cho khách hàng, giúp doanh nghiệp tăng doanh số và tăng cường sự phát triển.

1.7.1.4. Cách hoạt động của SPP

Cách hoạt động của SPP như sau:

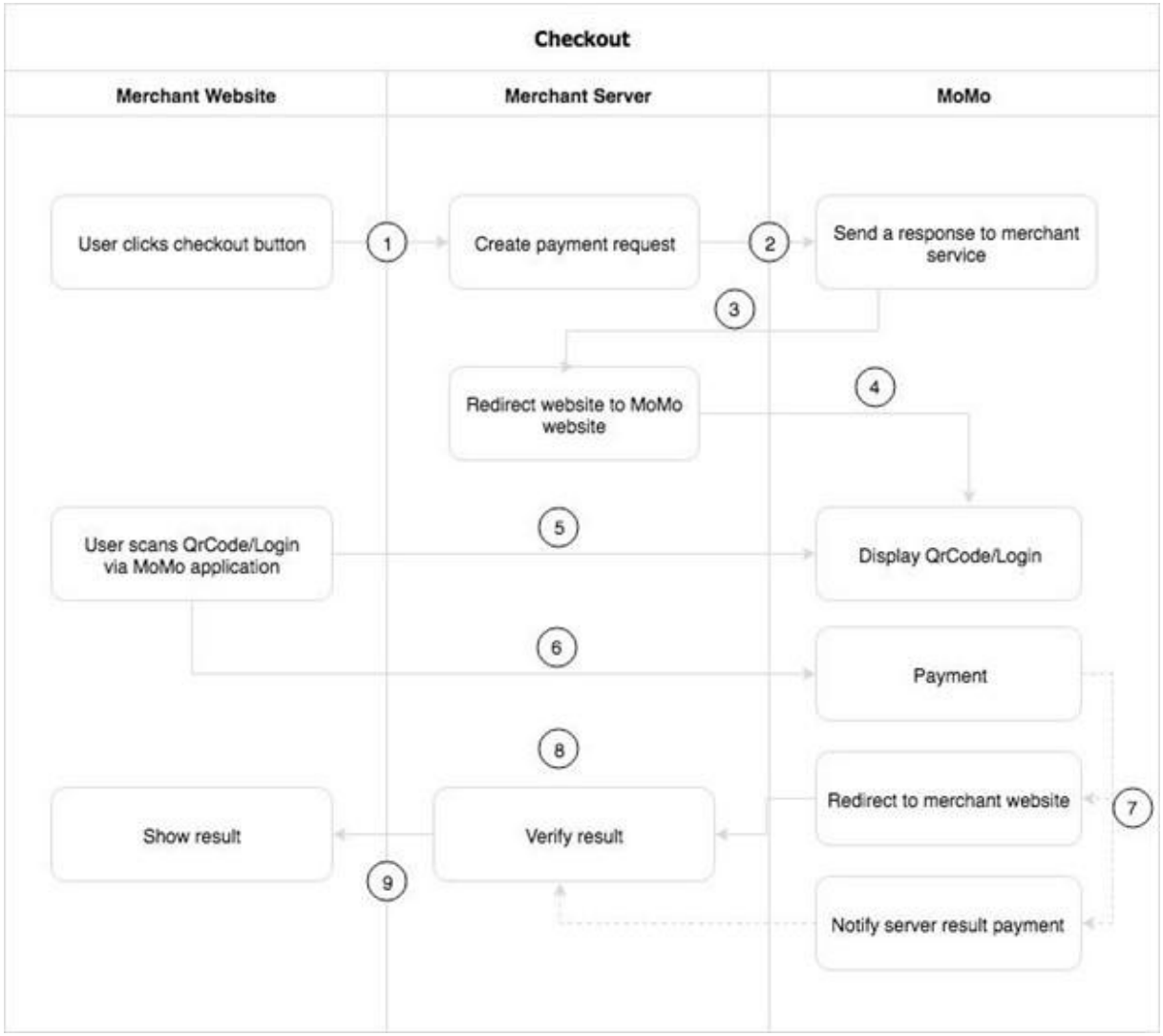
- Bước 1: Khởi tạo phiên giao dịch: Khách hàng khởi tạo phiên giao dịch bằng cách truy cập vào trang web của nhà bán hàng. Trong quá trình này, SPP sẽ tạo một mã phiên giao dịch duy nhất để xác định phiên giao dịch hiện tại.
- Bước 2: Yêu cầu thông tin thanh toán: Sau khi phiên giao dịch được khởi tạo, SPP sẽ yêu cầu thông tin thanh toán từ khách hàng. Ví dụ đối với thẻ credit/debit thì thông tin này bao gồm số thẻ tín dụng, ngày hết hạn của thẻ, mã bảo mật và số tiền cần thanh toán.
- Bước 3: Xác nhận thông tin thanh toán: Trong bước này, SPP sẽ kiểm tra tính hợp lệ của thông tin thanh toán được cung cấp bởi khách hàng bằng những phương pháp xác thực đặc thù. Nếu thông tin hợp lệ, SPP sẽ tiếp tục quá trình thanh toán, nếu không, SPP sẽ từ chối giao dịch này.
- Bước 4: Xác thực thanh toán: Sau khi xác nhận thông tin thanh toán hợp lệ, SPP sẽ tạo một yêu cầu xác thực thanh toán bằng cách gửi các thông tin liên quan đến

giao dịch cho ngân hàng của khách hàng. Ngân hàng sẽ tiến hành xác thực các thông tin này và phản hồi lại với SPP nếu giao dịch được chấp nhận hoặc từ chối.
- Bước 5: Hoàn tất giao dịch: Sau khi xác thực thanh toán thành công, SPP sẽ hoàn tất giao dịch và thông báo cho khách hàng và nhà bán hàng về kết quả giao dịch.

1.7.1.5. Ví dụ tích hợp thanh toán Momo

MoMo Payment Platform API là giải pháp thanh toán cho các đơn vị kinh doanh, cho phép khách hàng sử dụng tài khoản Ví MoMo để thanh toán các dịch vụ trên nhiều nền tảng khác nhau: Desktop Website, Mobile Website, Mobile Application, POS, Pay In Bill, Web In App MoMo.

Mô hình thanh toán:
- Bước 1: Khách hàng kiểm tra đơn hàng và chọn MoMo là phương thức thanh toán.
- Bước 2: Website bán hàng tạo session thanh toán và gửi yêu cầu thanh toán qua MoMo.
- Bước 3: Chuyển trang mua hàng sang trang thanh toán của MoMo.
- Bước 4: Khách hàng sử dụng ứng dụng MoMo để quét mã QR hoặc đăng nhập để thanh toán.
- Bước 5: Sau khi thanh toán MoMo sẽ chuyển khách hàng về trang mua hàng.
- Bước 6: Website bán hàng xác thực giao dịch và cập nhật dịch vụ cho khách hàng.



Hình 8: Sơ đồ xử lý thanh toán đơn hàng trên website desktop/mobile

Quy trình tích hợp:

- Đăng ký tài khoản doanh nghiệp. Cần hoàn thành quá trình đăng ký với đầy đủ thông tin, trạng thái mặc định của doanh nghiệp sẽ là chưa xác thực. Thông tin tích hợp mặc định sẽ môi trường Test.
- Tham khảo và lựa chọn phương thức thanh toán áp dụng cho dịch vụ của đơn vị kinh doanh.
- Tiến hành tích hợp theo tài liệu của từng phương thức thanh toán.
- Đơn vị tiến hành kiểm thử phần mềm, tham khảo các testcase của MoMo cung cấp để kiểm tra các lỗi phổ biến trong quá trình thanh toán.
- Sau khi đơn vị kinh doanh hoàn thành tích hợp và kiểm thử, MoMo sẽ xác thực dịch vụ trên môi trường test trước khi lên production.
- Sau khi được xác nhận, tài khoản doanh nghiệp sẽ được chuyển sang trạng thái đã xác thực.
- Thay đổi các thông tin tích hợp theo môi trường production.
- Triển khai dịch vụ thanh toán cho khách hàng.

Thông tin cấu hình để kết nối với MoMo API (Các thông tin này sẽ thay đổi theo từng môi trường):

- Partner Code: Thông tin để định danh tài khoản doanh nghiệp.
- Access Key: Cấp quyền truy cập vào hệ thống MoMo.
- Secret Key: Dùng để tạo chữ ký điện tử signature.
- Public Key: Sử dụng để tạo mã hoá dữ liệu bằng thuật toán RSA.

Cấu hình HTTP Request:

Key	**Value**
Content-Type	`application/json; charset=UTF-8`
Method	POST
Domain	Production: https://payment.momo.vn Sandbox: https://test-payment.momo.vn

Bảng 1: Cấu hình HTTP

Địa chỉ IP (Internet Protocol):

Môi trường	**Incoming**	**Outcoming**
Sandbox	210.245.113.71	118.69.210.244
Production	118.69.212.158	118.69.210.244

Bảng 2: Địa chỉ IP

MoMo sử dụng chữ ký điện tử và mã hoá dữ liệu để xác thực dữ liệu đầu vào và ra trên mỗi yêu cầu HTTP Request/HTTP Response. Thư viện thuật toán sử dụng Hmac_SHA, RSA.

Chữ ký điện tử: “signature” là một chuỗi ký tự được tạo ra từ một thuật toán cho trước, sử dụng để kiểm tra tính đúng đắn của dữ liệu trên đường truyền giữa 2 hệ thống. Một số thuật toán đang sử dụng là MD5, SHA1, SHA256 và Hmac. MoMo sử dụng thuật toán HMAC_SHA256 để tạo signature. Dữ liệu đầu vào bao gồm secret key và data, data được tạo ra theo định dạng:

`key1=value1&key2=value2... (key1: tên field, value1 = giá trị của key1)`

Hình 9: Ví dụ request mẫu

Cách tạo chữ ký điện tử:

```
partnerCode=$partnerCode&accessKey=$accessKey&requestId=
$requestId&amount=$amount&orderId=$orderId&orderInfo=$or
derInfo&returnUrl=$returnUrl&notifyUrl=$notifyUrl&extraD
ata=$extraData
```

Dữ liệu được tạo ra:

```
partnerCode=MOMO&accessKey=F8BBA842ECF85&requestId=MM154
0456472575&amount=150000&orderId=MM1540456472575&orderIn
fo=SDK_team.&returnUrl=https://momo.vn&notifyUrl=https:/
/momo.vn&extraData=email=abc@gmail.com
```

Chữ ký được tạo ra: `K951B6PE1waDMi640xX08PD3vg6EkVlz`

Mã hóa RSA: Mã hóa RSA là một thuật toán mã hóa khóa công khai để bảo vệ thông tin trên đường truyền. Sử dụng một cặp key (public key và private key) để mã hóa và giải mã dữ liệu. Đối tác dùng public key do MoMo cung cấp để mã hóa data theo định dạng của MoMo, MoMo sẽ giải mã bằng private key. Thuật toán RSA được MoMo sử dụng theo chuẩn PKCS.

Hình 10: Dữ liệu trước khi hash bằng RSA

Dữ liệu sau khi RSA:

```
A7WFmmnpn6TRX42Akh/iC5DdU5hhBT9LR5QSG6rJAl7
0hfEkkGUx2pTCai8s+M9KMVUcJ7m52iv74yhmeEjjN1
0TtEJoqITBIYBG2bqcTprhDijyhV4ePU7ytDNuLxzzI
vGfTYyvbsEJ2jZTSf556yod12vhYqOJSFL/U2hVuxjU
ahf5Rnu5R/OLalg8QmlU6nQooEuNdzEXPMd6j9EaxOC
iB2oM5/9QiTN0tCNSTIVvPtnlHu5mIbBHChcwfToIL4
IAiD1nbrlDuBX//CZcrZj6hFqjvU31yb/DuG02c3aqW
xbZKZ8csOwF9bL30m/yGr/0BQUWgunpDPrmCosf9A==
```

Tạo đơn thanh toán Momo: Ở trên trang thanh toán của website bán hàng, sau khi khách hàng lựa chọn sản phẩm hoặc dịch vụ và nhấn chọn thanh toán bằng ví điện tử MoMo. Website bán hàng cần gọi tới API tạo đơn thanh toán Momo kèm theo dữ liệu của đơn hàng.

Attribute	Type	Required	Description
partnerCode	String	√	Thông tin tích hợp
partnerName	String		Tên đối tác
storeId	String		Thông tin cửa hàng
requestId	String	√	Định danh mỗi yêu cầu
amount	Long	√	Số tiền cần thanh toán Min: 1.000 VND Max: 20.000.000 VND Tiền tệ: `VND` Kiểu dữ liệu: `Long`
orderId	String	√	Mã đơn hàng thanh toán của đối tác
orderInfo	String	√	Thông tin đơn hàng
autoCapture	Boolean		Nếu giá trị false, giao dich sẽ không tự động `capture` , Mặt định là true
redirectUrl	String	√	Một URL của đối tác. URL này được sử dụng để chuyển trang (redirect) từ MoMo về trang mua hàng của đối tác sau khi khách hàng thanh toán. Hỗ trợ: **AppLink** và **WebLink**
ipnUrl	String	√	API của đối tác. Được MoMo sử dụng để gửi kết quả thanh toán theo phương thức IPN (server-to-server)
requestType	String	√	`captureWallet`
extraData	String	√	Giá trị mặc định là trống `""` Encode base64 theo định dạng Json: `{"key": "value"}` Ví dụ với dữ liệu: `{"username": "momo"}` thì data của `extraData` là `eyJ1c2VybmFtZSI6ICJtb21vIn0=`
lang	String	√	Ngôn ngữ của `message` được trả về (`vi` hoặc `en`)
signature	String	√	Chữ ký. Sử dụng thuật toán `Hmac_SHA256` với data theo định dạng được sort từ a-z : **HMAC_SHA256** `(accessKey=$accessKey&amount=$amount&extraData=$extraData&ipnUrl=$ipnUrl&orderId=$orderId&orderInfo=$orderInfo&partnerCode=$partnerCode&redirectUrl=$redirectUrl&requestId=$requestId&requestType=$requestType,` **secretKey** `)`

Hình 11: Định nghĩa các trường dữ liệu của Redirect HTTP request

```json
{
  "partnerCode": "MOMO",
  "partnerName" : "Test",
  "storeId" : "MomoTestStore",
  "requestType": "captureWallet",
  "ipnUrl": "https://momo.vn",
  "redirectUrl": "https://momo.vn",
  "orderId": "MM1540456472575",
  "amount": 150000,
  "lang":  "vi",
  "orderInfo": "SDK team.",
  "requestId": "MM1540456472575",
  "extraData": "eyJ1c2VybmFtZSI6ICJtb21vIn0=",
  "signature": "fd37abbee777e13eaa0d0690d184e4d7e2fb43977281ab0e20701721f07a0e07"
}
```


Hình 12: Ví dụ các trường dữ liệu của Redirect HTTP request

HTTP response trả về trạng thái tạo đơn hàng kèm link chuyển hướng sang trang thanh toán phía Momo để khách hàng tiến hành thanh toán, định nghĩa các trường thông tin như sau:

Attribute	Type	Required	Description
partnerCode	String	√	Thông tin tích hợp
requestId	String	√	Giống với yêu cầu ban đầu
orderId	String	√	Mã đơn hàng của đối tác
amount	Long	√	Giống với số tiền yêu cầu ban đầu
responseTime	Long	√	Thời gian trả kết quả thanh toán về đối tác Định dạng: `timestamp`
message	String	√	Mô tả lỗi dựa trên `lang`
resultCode	int	√	Mã lỗi
payUrl	String	√	URL để chuyển từ trang mua hàng của đối tác sang trang thanh toán của MoMo
deeplink	String		URL để mở ứng dụng trực tiếp MoMo (Khách hàng phải cài đặt ứng dụng MoMo trước) và trang xác nhận thanh toán.
qrCodeUrl	String		Dữ liệu để tạo mã QR nếu bạn muốn khách hàng quét mã QR trực tiếp trên trang mua hàng hoặc in mã lên hoá đơn. `Lưu ý` : Đây không phải URL chứa hình ảnh của mã QR, bạn cần sử dụng thư viện ngoài để tạo mã QR.
deeplinkMiniApp	String		URL mở màn hình xác nhận thanh toán của ứng dụng MoMo. Áp dụng khi đối tác sử dụng mini app nhúng vào trong ứng dụng MoMo

Hình 13: Định nghĩa các trường thông tin của HTTP response trả về

Sau khi khách hàng tiến hành thanh toán, phía Momo đã xác thực thanh toán và đã thanh toán xong thì sẽ redirect tiếp đến "redirectUrl" đã được định nghĩa trong HTTP response bên trên, kèm theo HTTP request body data như sau:

```
redirectUrl?{your_parameters}&partnerCode=$partnerCode&
orderId=$orderId&requestId=$requestId&amount=$amount&or
derInfo=$orderInfo&orderType=momo_wallet&transId=$trans
Id&resultCode=$resultCode&message=$message&payType=$pay
Type&responseTime=$responseTime&extraData=$extraData&si
gnature=$signature
```

1.7.2. Ứng dụng của Secure Payment Protocols trong Laravel Web Framework

1.7.2.1. Giới thiệu Laravel

Laravel là một framework mã nguồn mở và phổ biến cho phát triển ứng dụng web dựa trên PHP. Laravel được phát triển bởi Taylor Otwell vào năm 2011, và hiện nay đang là một trong những framework phổ biến nhất cho phát triển web với PHP. Laravel được thiết kế để mang lại sự đơn giản và dễ sử dụng cho việc phát triển ứng dụng web. Nó cung cấp rất nhiều tính năng, công cụ và thư viện hữu ích cho việc phát triển ứng dụng web, bao gồm:

- Mô hình MVC (Model-View-Controller): Giúp tách biệt các thành phần của ứng dụng, tăng tính linh hoạt và khả năng bảo trì.
- Routing: Giúp định tuyến các yêu cầu từ trình duyệt đến các controller và hành động tương ứng.
- Blade: Một hệ thống mẫu gọn nhẹ, dễ sử dụng cho phép tạo các giao diện người dùng đẹp và hiệu quả.
- Eloquent ORM: Cho phép tương tác với cơ sở dữ liệu một cách dễ dàng và hiệu quả.
- Artisan Command Line Interface: Cung cấp một bộ công cụ dòng lệnh để hỗ trợ phát triển ứng dụng.
- Laravel Mix: Cung cấp một cách dễ dàng để tổng hợp các tài nguyên web, bao gồm CSS, JavaScript và hình ảnh.

Ngoài ra, Laravel còn có nhiều tính năng khác như bảo mật, phân quyền, xử lý file, gửi email, xử lý định lượng, tương tác với API, và nhiều hơn nữa.

Với những tính năng và công cụ mạnh mẽ, Laravel trở thành một trong những lựa chọn hàng đầu cho phát triển ứng dụng web PHP.

1.7.2.2. Sử dụng SPP trong Laravel

Laravel cung cấp một số tính năng để hỗ trợ việc tích hợp các hình thức thanh toán trực tuyến vào ứng dụng web và SPP là một trong số đó.

Để sử dụng SPP trong Laravel, trước hết ta cần phải cài đặt một số thư viện cần thiết. Laravel hỗ trợ nhiều thư viện khác nhau để hỗ trợ thanh toán trực tuyến. Một trong những thư viện được sử dụng phổ biến nhất để hỗ trợ thanh toán trực tuyến trong Laravel là Omnipay. Omnipay là một thư viện được thiết kế để hỗ trợ nhiều cổng thanh toán khác nhau và cung cấp một giao diện thân thiện cho việc xây dựng các hình thức thanh toán trực tuyến trong ứng dụng.

Để sử dụng SPP với Omnipay, cần cài đặt Omnipay-SecurePay thư viện để hỗ trợ SPP. Sau khi cài đặt thành công thư viện có thể bắt đầu tích hợp SPP vào ứng dụng Laravel của mình.

Bước đầu tiên là cấu hình SPP trong tệp .env của ứng dụng Laravel. Ta cần cung cấp các thông tin về tài khoản SPP, bao gồm merchant ID, merchant key và merchant password. Ta cũng có thể cấu hình môi trường thanh toán (sandbox hoặc production) trong tệp .env.

Sau khi cấu hình SPP, ta có thể sử dụng Omnipay để tạo các đối tượng thanh toán và thực hiện các giao dịch thanh toán trực tuyến. Ví dụ, sau đây là một ví dụ về việc sử dụng Omnipay để thanh toán thông qua SPP trong Laravel:

```
use Omnipay\Omnipay;

$gateway = Omnipay::create('SecurePay_DirectPost');
$gateway->setMerchantId(env('SPP_MERCHANT_ID'));
$gateway->setMerchantKey(env('SPP_MERCHANT_KEY'));
$gateway->setPassword(env('SPP_MERCHANT_PASSWORD'));
$gateway->setTestMode(env('SPP_TEST_MODE'));

$response = $gateway->purchase([
  'amount' => '10.00',
  'currency' => 'AUD',
  'card' => [
    'number' => '4111111111111111',
```

Trong ví dụ trên, chúng ta tạo một đối tượng gateway sử dụng thư viện Omnipay và thiết lập thông tin tài khoản SPP của chúng ta. Chúng ta sau đó tạo một giao dịch thanh toán với một số thông tin cơ bản, bao gồm số tiền, đơn vị tiền tệ và thông tin thẻ thanh toán. Chúng ta gửi giao dịch thanh toán đến SPP thông qua đối tượng gateway và kiểm tra kết quả trả về để xác định xem thanh toán có thành công hay không.

1.8. Kết chương

Mục tiêu của nghiên cứu này là tìm hiểu về Secure Payment Protocol (SPP) và cách tích hợp SPP vào ứng dụng Laravel để đảm bảo an toàn và bảo mật trong quá trình thanh toán trực tuyến. SPP là một giao thức thanh toán quan trọng và được sử dụng rộng rãi trong thương mại điện tử hiện nay. Tích hợp SPP vào ứng dụng Laravel không quá phức tạp với sự hỗ trợ của các thư viện và công cụ như Omnipay và Composer. Việc tích hợp SPP sẽ giúp ứng dụng đạt được một số lợi ích quan trọng, bao gồm:

- Bảo mật: SPP đảm bảo rằng các giao dịch thanh toán được mã hóa và bảo mật trong suốt quá trình truyền tải.
- Đa nền tảng: SPP có thể hoạt động trên nhiều nền tảng khác nhau, bao gồm web và mobile.
- Tích hợp dễ dàng: Các thư viện như Omnipay giúp tích hợp SPP vào ứng dụng Laravel của mình một cách dễ dàng.

Tuy nhiên, khi tích hợp SPP vào ứng dụng cần lưu ý một số vấn đề quan trọng, bao gồm:

- Bảo mật thông tin tài khoản: Cần bảo mật thông tin tài khoản của mình và không chia sẻ với bất kỳ ai khác.
- Kiểm tra tính hợp lệ của đơn hàng: Cần kiểm tra tính hợp lệ của các đơn hàng trước khi thực hiện giao dịch thanh toán, để đảm bảo rằng chỉ các đơn hàng hợp lệ mới được thanh toán.
- Xử lý lỗi: Cần xử lý các lỗi xảy ra trong quá trình thanh toán để đảm bảo rằng người dùng nhận được thông báo hợp lý nếu có lỗi xảy ra.

Tích hợp SPP vào ứng dụng Laravel là một bước quan trọng để đảm bảo an toàn và bảo mật trong quá trình thanh toán trực tuyến cần chú ý các vấn đề an toàn và bảo mật liên quan đến thông tin tài khoản và đơn hàng, và xử lý các lỗi một cách hợp lý để đảm bảo rằng người dùng nhận được trải nghiệm thanh toán trực tuyến tốt nhất.

Trong chương 1 đã tìm hiểu về thương mại điện tử, website thương mại điện tử, các yếu tố quan trọng để thiết kế thương mại điện tử và tìm hiểu các lỗi bảo mật phổ biến mới nhất hiện nay cũng như các giải pháp xác thực an toàn cho dữ kiệu thanh toán. Từ những phần tìm hiểu này cho thấy việc xây dựng 1 trang website thương mại điện tử an toàn với doanh nghiệp cũng như khác hàng sử dụng là vô cùng quan trọng. Phần tiếp theo của đồ án sẽ nói về phân tích và thiết kế website thương mại điện tử xây dựng dưa trên việc khảo sát và xác định yêu cầu ở Chương 1.

CHƯƠNG 2. PHÂN TÍCH VÀ THIẾT KẾ WEBSITE TMĐT

2.1. Mô tả bài toán

2.1.1. Phân tích bài toán

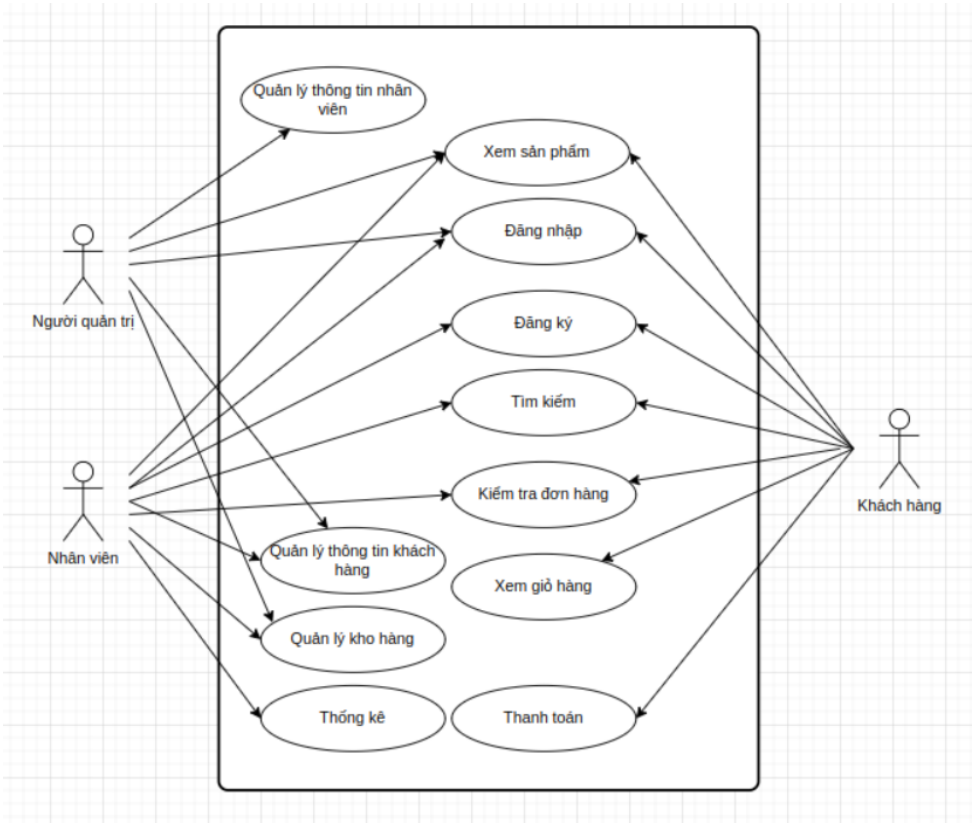
Công ty ABC kinh doanh về lĩnh vực may mặc muốn xây dựng hệ thống website thương mại điện tử với các yêu cầu:

- Giao diện quản lý đơn giản dễ sử dụng, giao diện người dùng dễ nhìn, đặt hàng nhanh chóng
- Có chatbot, có biểu đồ quản lý thống kê theo ngày tháng năm
- Chức năng gửi thông báo về email
- Nhiều dịch vụ thanh toán
- Đăng ký tài khoản dễ dàng
- …

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.

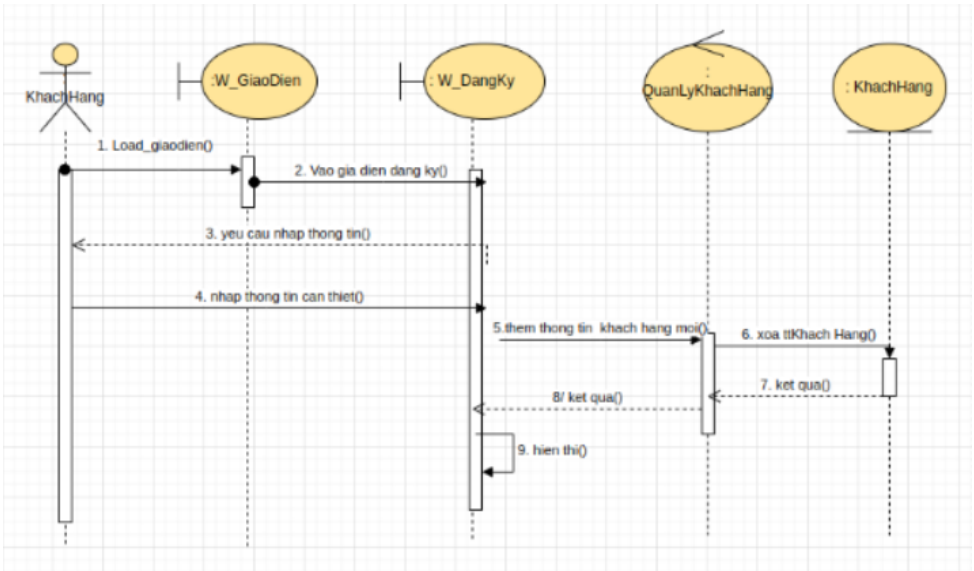
2.2. Phân tích nghiệp vụ và yêu cầu chức năng



Hình 14: Biểu đồ usecase tổng quát

2.2.1. Chức năng 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.



Hình 15: Biểu đồ trình tự đăng ký

2.2.2. Chức năng đăng nhập

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.

2.2.3. 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.

2.2.4. 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.

2.2.5. 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] “OWASP top 10 vulnerabilities 2023.” [Online]. Available: https://www.edudwar.com/owasp-top-10-vulnerabilities/