HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

NGUYỄN XUÂN GIANG

NGHIÊN CỨU GIẢI PHÁP BẢO MẬT WEBSITE CHO CÁC DOANH NGHIỆP VỪA VÀ NHỎ

CHUYÊN NGÀNH: **HỆ THỐNG THÔNG TIN**
MÃ SỐ: **8.48.01.04**

TÓM TẮT LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

NGƯỜI HƯỚNG DẪN KHOA HỌC: PGS.TS. LÊ HỮU LẬP

HÀ NỘI - 2021

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: **PGS.TS. LÊ HỮU LẬP**

Phản biện 1: PGS. TS. Nguyễn Đức Dũng

Phản biện 2: PGS. TS. Hoàng Hữu Hạnh

Luận văn sẽ được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: 14 giờ 00 ngày 28 tháng 8 năm 2021

Có thể tìm hiểu luận văn tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông

MỞ ĐẦU

Trong thời đại công nghiệp 4.0, vấn đề an ninh mạng ngày càng trở nên nóng bỏng với hàng loạt vụ tấn công nhằm vào các website của các cơ quan nhà nước và doanh nghiệp, đặc biệt là những doanh nghiệp vừa và nhỏ. Theo số liệu của Tổng cục Thống kê, tính đến hết năm 2020, cả nước có khoảng 900 nghìn doanh nghiệp đang hoạt động, trong đó, số lượng doanh nghiệp vừa, nhỏ và siêu nhỏ chiếm 98%. Đây sẽ là mảnh đất màu mỡ cho các hacker tấn công, làm ngừng trệ các dịch vụ dựa trên nền tảng website, gây ảnh hưởng nghiêm trọng đến kinh tế, uy tín và hoạt động điều hành của các cơ quan nhà nước và doanh nghiệp.

Các chuyên gia bảo mật đã liệt kê một số cách mà việc bị tin tặc tấn công có thể gây hại cho các cơ quan nhà nước cũng như các doanh nghiệp như sau [24]:

** Mất lưu lượng truy cập.*

Đây là một vấn đề vô cùng quen thuộc nhưng vẫn chưa bao giờ bớt nghiêm trọng. Cùng với việc các doanh nghiệp tập trung vào nền tảng online của họ để đảm bảo trải nghiệm tiện lợi và kết nối với người dùng hiệu quả, thời gian website ngừng hoạt động có thể tương đương với những tổn thất vô cùng lớn. Do bản chất liên tục được truy cập bởi người dùng, các doanh nghiệp mua sắm trực tuyến đặc biệt cần chú ý trang bị giải pháp giám sát và bảo vệ hợp lý.

Mất lưu lượng truy cập có thể do những lý do khác nhau, điển hình là do bị liệt vào danh sách đen của các bộ máy tìm kiếm do chứa mã độc. Google thực hiện việc này bằng cách hiện dòng chữ "trang web này có thể bị hack" bên cạnh kết quả tìm kiếm kèm với thông báo bảo mật toàn màn hình khi người dùng click vào. Với nhiều website, lượng tiếp cận tự nhiên hầu như đến từ các bộ máy tìm kiếm. Việc bị "chỉ điểm" bởi các bộ máy tìm kiếm sẽ khiến một lượng lớn người dùng rời khỏi website mà họ đang định truy cập.

** Lây lan malware sang máy tính người dùng.*

Với sự bùng nổ của tiền ảo và công nghệ blockchain trong những năm gần đây, cộng đồng mạng đã chứng kiến những biến thể vô cùng mới mẻ đang gia nhập vào kho malware toàn cầu: malware đào tiền ảo. Loại malware này khi bị chèn vào website sẽ ngầm dùng CPU của người dùng để đào đồng tiền ảo Monero và các loại tiền ảo khác cho tin tặc.

Điều xảy ra tiếp theo là mỗi khi người dùng truy cập website đó, máy tính của họ sẽ đột ngột chậm đi hoặc họ sẽ được trình diệt virus cảnh báo về mã độc tồn tại trên website. Trong

trường hợp người đó không có trình duyệt virus trong máy tính, chính website này sẽ chịu trách nhiệm cho việc để lây lan malware sang thiết bị của họ.

** Mất uy tín thương hiệu.*

Đây là vấn đề thật sự lớn. Sau khi tìm hiểu về những vấn đề trên, hẳn chúng ta đã có cái nhìn rõ hơn rằng nếu website không được thực hiện bảo mật một cách hiệu quả, người dùng sẽ nhanh chóng nắm được. Họ sẽ được cảnh báo bởi bộ máy tìm kiếm, các ứng dụng diệt virus và phần mở rộng trình duyệt. Trải nghiệm của họ với website sẽ không hề tích cực.

Điều gì sẽ xảy ra nếu dữ liệu của các cơ quan, các doanh nghiệp, bị mất vào tay tin tặc? Uy tín của những đơn vị này sẽ bị ảnh hưởng nghiêm trọng. Còn nếu chúng ta không may trở thành nạn nhân của một vụ lộ thông tin nhạy cảm - như thông tin thanh toán - xử lý rủi ro sẽ vô cùng khó khăn và tốn kém.

** Tốn kém chi phí.*

Chốt lại, tổn thất của mỗi hệ quả của việc bị hack website có thể được đo bằng những khoản phí tổn. Phí dọn sạch malware và phục hồi dữ liệu mới chỉ là bước đầu. Các chiến dịch marketing sẽ phải bị hủy bỏ. Nguồn lực và thời gian sẽ bị lãng phí. Lợi nhuận sẽ sa sút nghiêm trọng. Khách hàng sẽ rời bỏ dịch vụ. Tổng chi phí dành cho các cuộc tấn công mạng trên toàn cầu đã đạt tới con số 100 tỉ đô la Mỹ.

Như đã nói ở trên, tin tặc có động lực về lợi nhuận khi thực hiện hack website. Với động lực đó, có thể khẳng định tội phạm mạng sẽ còn tăng trưởng theo cấp số nhân trong thời gian tới.

Thực tế cho thấy việc bảo mật website ở những doanh nghiệp vừa và nhỏ hiện nay đang tồn tại những yếu kém, vấn đề an toàn bảo mật chưa được quan tâm đúng mức. Có rất nhiều lí do khiến cho tình trạng bảo mật website còn yếu kém ở Việt Nam nói chung và các doanh nghiệp vừa vả nhỏ nói riêng. Dưới đây là một số lí do chính:

Thứ nhất: nguồn nhân lực công nghệ thông tin mỏng, đặc biệt là chưa có hoặc rất ít đơn vị có chuyên viên bảo mật phụ trách riêng

Thứ hai: Sự nhận thức hạn chế về an toàn bảo mật của người sử dụng

Thứ ba: Chỉ coi trọng việc đăng tin và truy cập được đến website, chưa coi trọng việc phát hiện và phòng ngừa điểm yếu của website

Thứ tư: không rà quét thường xuyên các lỗ hổng bảo mật của website và hạ tầng công nghệ thông tin của đơn vị

Thứ năm: Không cập nhật thường xuyên các bản vá lỗi cho website, cho hệ thống thông tin của đơn vị

Vì vậy, vấn đề nghiên cứu các giải pháp bảo mật website có tính cấp thiết, có ý nghĩa khoa học và thực tiễn. Từ nhu cầu phát triển, đòi hỏi các cơ quan, tổ chức, doanh nghiệp phải có biện pháp đảm bảo an toàn cho website của mình.

Từ những lý do trên và đặc thù công việc quản lý nhà nước tại Sở Thông tin và Truyền thông Hà Nội, học viên đã chọn đề tài **"Nghiên cứu giải pháp bảo mật website cho các doanh nghiệp vừa và nhỏ"** cho luận văn tốt nghiệp trình độ đào tạo thạc sỹ.

*** Mục đích nghiên cứu:**

Mục đích chính của luận văn là nghiên cứu các giải pháp bảo mật website và đánh giá mức độ bảo mật của một website bất kỳ.

*** Đối tượng và phạm vi nghiên cứu:**

- Đối tượng nghiên cứu của luận văn là các ứng dụng website và các vấn đề liên quan đến bảo mật website.

- Phạm vi nghiên cứu của luận văn là: các giải pháp bảo mật website và đánh giá mức độ bảo mật của một website bất kỳ.

*** Phương pháp nghiên cứu:**

- Về mặt lý thuyết: thu thập, khảo sát, phân tích các tài liệu và thông tin có liên quan đến các bảo mật website.

- Về mặt thực nghiệm: khảo sát thực tế và đánh giá mức độ bảo mật của một website bất kỳ.

Bố cục của luận văn gồm 3 chương chính với các nội dung sau:

Chương 1: Tổng quan bảo mật Website

Nội dung của chương 1 là tìm hiểu các lỗi bảo mật và các phương thức tấn công website của hacker.

Chương 2: Các giải pháp đảm bảo an toàn thông tin của Website

Nội dung của chương 2 luận văn tập trung nghiên cứu các giải pháp đảm bảo an toàn thông tin của website, trong đó đi sâu vào biện pháp tấn công từ chối dịch vụ.

Chương 3: Đánh giá mức độ bảo mật website của Sở Thông tin và Truyền thông Hà Nội

Chương 3 của luận văn tiến hành đánh giá mức độ bảo mật website Sở Thông tin và Truyền thông Hà Nội và đưa ra các giải pháp nâng cao bảo mật.

CHƯƠNG 1. TỔNG QUAN VỀ BẢO MẬT WEBSITE

Nội dung của Chương 1 sẽ tìm hiểu các lỗi bảo mật và các phương thức tấn công website của hacker.

1.1. Một số loại website phổ biến

1.1.1. Phân loại theo cấu trúc website

Website tĩnh (static website): Website tĩnh ở đây được hiểu theo nghĩa là dữ liệu website không được thay đổi thường xuyên. Loại website này được lập trình dựa trên nền tảng HTML, CSS và Javascript. Nếu muốn thay đổi nội dụng trên website, quản trị viên phải sửa đổi trực tiếp trên mã lệnh và chỉ những người am hiểu về ngôn ngữ lập trình mới có thể thực hiện thao tác này. Chính vì thế mà website tĩnh hiện nay không được sử dụng phổ biến.

Website động (dynamic website): Hầu hết các website hiện nay đều thuộc cấu trúc website động. Khác với website tĩnh, website động luôn luôn có thông tin mới do các thông tin này được cập nhật thường xuyền bởi các quản trị viên. Các thông tin mới này được lưu vào cơ sở dữ liệu của website và đưa ra sử dụng dựa theo yêu cầu của người dùng. Hiện nay có nhiều ngôn ngữ lập trình được sử dụng để lập trình các website động như HTML, CSS, Javascript, PHP hay ASP.NET…

1.1.2. Phân loại theo chức năng

1.1.2.1. Trang website thương mại điện tử

1.1.2.2. Website landing page giới thiệu sản phẩm

1.1.2.3. Trang website giải trí

1.1.2.4. Website tin tức

1.1.2.5. Mạng xã hội

1.1.2.6. Website diễn đàn

1.1.2.7. Website rao vặt

1.1.2.8. Website cổng thông tin điện tử của tổ chức nhà nước, chính phủ, trường học, bệnh viện

1.1.3. Phân loại theo quyền sở hữu

Website doanh nghiệp: là trang web đại diện cho một doanh nghiệp cụ thể. Website được tạo ra với mục đích giới thiệu doanh nghiệp, cập nhật thông tin hoạt động, quảng bá sản phẩm dịch vụ và còn rất nhiều chức năng khác. Tất cả các đơn vị đều có nhu cầu quảng bá hình ảnh của mình nên website doanh nghiệp được xem là một phần không thể thiếu đối với các công ty hiện nay. Ví dụ website của công ty sữa Vinamilk: https://www.vinamilk.com.vn

Website cá nhân: Khác với trang web doanh nghiệp, website cá nhân chỉ thuộc quyền sở hữu của một người nào đó. Loại website này chỉ phổ biến với người của công chúng, những người cần quảng bá hình ảnh cá nhân để phục vụ cho mục đích thương mại hay công việc. Chẳng hạn như: chính trị gia, ca sĩ, nhà thiết kế, nhà văn, nhà thuyết giảng…

1.1.4. Phân loại theo tính bảo mật

1.1.4.1. Website cần tính bảo mật thấp

Những trang web được liệt kê vào phân loại này thường là những website tĩnh hoặc các landing page, chỉ có mục đích cung cấp thông tin về sản phẩm, dịch vụ của doanh nghiệp.

Những trang web dạng này thường không khắt khe về tính bảo mật vì những thông tin cung cấp không mang tính chất nhạy cảm.

1.1.4.2. Website cần tính bảo mật trung bình

Những trang web ở loại này thường là những website chỉ cung cấp thông tin giải trí, tin tức thông thường như trang thông tin điện tử tổng hợp hoặc blog cá nhân.

Những thông tin cần bảo mật ở những website này chỉ là những thông tin về hình ảnh, bài viết của chính website.

1.1.4.3. Website cần tính bảo mật cao

Đây thường là những website cung cấp các dịch vụ như mua bán hàng hóa, cung cấp thông tin cá nhân, doanh nghiệp. Có thể liệt kê các website thương mại điện tử, các diễn đàn, mạng xã hội nhỏ.

Những thông tin của khách hàng như thông tin cá nhân, thông tin thanh toán, hình ảnh cá nhân đều mang tính chất nhạy cảm do đó những trang web này cần tính bảo mật cao.

Đảm bảo không để rò rỉ thông tin quan trọng, tạo cơ hội cho hacker tấn công gây thiệt hại cho khách hàng và doanh nghiệp.

1.1.4.4. Website cần tính bảo mật rất cao

Những website yêu cầu tính bảo mật rất cao thường là những website thuộc các tổ chức chính phủ, nhà nước. Những thông tin là phát ngôn của tổ chức nhà nước nếu bị tin tặc tấn công gây sai lệch sẽ gây ra những hậu quả vô cùng nghiêm trọng.

Bên cạnh đó những mạng xã hội với lượng người dùng rất lớn như facebook, twitter, youtube, zalo cũng là những website cần tính bảo mật rất cao. Vì lượng thông tin cá nhân rất lớn lên đến hàng triệu, hàng tỉ thông tin cá nhân. Nếu bị tin tặc tấn công và lợi dụng cũng sẽ gây ra những thiệt hại vô cùng lớn.

1.2. Tình hình tấn công website trên thế giới và Việt Nam

Trong 9 tháng đầu năm 2020, báo cáo mới được công bố đã ghi nhận xu hướng tích cực của an ninh website trên toàn cầu. Cụ thể, hệ thống CyStack Attack Map ghi nhận 343.365 vụ tấn công vào website, giảm 24,7% so với cùng kỳ năm trước.

Cũng theo báo cáo, châu Á đang là điểm nóng thứ hai, chỉ sau Mỹ khi xét tới số vụ tấn công website với 113.913 vụ, tương đương 33,2% tổng số vụ tấn công trên toàn cầu.

Như vậy, trong 9 tháng đầu năm 2020, châu Á đi ngược lại xu hướng giảm của thế giới khi số vụ tấn công website tăng 4,1% so với cùng kỳ năm 2019.

Tại Việt Nam, các hệ thống mạng và website bị tấn công theo chiều hướng gia tăng hàng năm, không chỉ về số lượng mà các phương pháp tấn công cũng liên tục được hoàn thiện:

- Năm 2019: Theo thống kê của của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT), trong năm 2019, trung tâm đã ghi nhận 6.219 sự cố tấn công mạng vào các trang web của Việt Nam. Trong đó có 2.155 sự cố tấn công lừa đảo (Phishing), 3.824 trường hợp sự cố tấn công thay đổi giao diện (Deface) và 240 sự cố website bị nhiễm mã độc (Malware). So với cùng kỳ năm 2018, tổng số sự cố tấn công tăng 104%. Cụ thể, từng loại tấn công tăng giảm như sau: Phishing tăng 141%, deface tăng 109%, riêng malware giảm 26,57%. Bên cạnh đó, hàng ngày có khoảng gần 100.000 địa chỉ mạng của Việt Nam truy vấn hoặc kết nối mạng lưới máy tính ma (botnet).

- Năm 2020: Đại dịch Covid-19 bùng phát, hàng loạt doanh nghiệp, cơ quan, tổ chức chuyển sang làm việc từ xa. Các phần mềm làm việc trực tuyến được tìm kiếm và download

rầm rộ. Nhiều đơn vị buộc phải mở hệ thống ra internet để nhân viên có thể truy cập và làm việc từ xa… Điều này tạo môi trường cho kẻ xấu khai thác lỗ hổng, tấn công, đánh cắp thông tin.

Theo báo cáo an ninh mạng website trong 9 tháng đầu năm 2020 do Công ty an toàn thông tin CyStack công bố (Là báo cáo thống kê và phân tích tình hình tấn công website trên toàn thế giới, báo cáo an ninh website được CyStack thực hiện định kỳ hàng quý. Dữ liệu trong báo cáo này được trích xuất từ hệ thống CyStack Attack Map do CyStack nghiên cứu và phát triển), hệ thống đã ghi nhận 343.365 vụ tấn công vào website trên toàn thế giới. Trong đó, châu Á đang là điểm nóng thứ hai, chỉ sau Mỹ với 113.913 vụ tấn công website, tương đương 33,2% tổng số vụ tấn công trên toàn cầu, tăng 4,1% so với cùng kỳ năm 2019.

Trong năm 2020, nhờ thực hiện nhiều biện pháp phòng chống tấn công mạng, Việt Nam đã cải thiện đáng kể tình hình an ninh website so với năm 2019. Cụ thể, số cuộc tấn công trong ba quý đầu năm 2020 đã giảm 64,8% so với cùng kỳ năm 2019, từ 8418 về mức 3041 vụ. Tổng kết 9 tháng đầu năm 2020, Việt Nam đứng thứ 18 trên bản đồ tấn công website toàn cầu. Xét trong 5 quý gần nhất, Việt Nam đã cải thiện đáng kể an ninh mạng website, đặc biệt là quý I/2020 với chỉ 838 vụ và xếp thứ 19 trên thế giới. Số lượng cuộc tấn công website tại Việt Nam tăng nhẹ trong quý II và quý III lần lượt là 27,3% và 7,5% so với quý trước đó.

1.3. Các lỗi bảo mật phổ biến của ứng dụng web và nguy cơ mất an toàn thông tin của các doanh nghiệp

Lỗ hổng 1: Lỗ hổng XSS

Lỗ hổng 2: Chèn mã độc hại (Injection flaws)

Lỗ hổng 3: Tệp tin chứa mã độc

Lỗ hổng 4: CSRF

Lỗ hổng 5: Tham chiếu đối tượng trực tiếp không an toàn

Lỗ hổng 6: Rò rỉ thông tin và xử lý lỗi không đúng cách

Lỗ hổng 7: Quản lý xác thực và quản lý phiên yếu

Lỗ hổng 8: Không hạn chế truy nhập vào URL nội bộ

Lỗ hổng 9: Không kiểm tra sự điều hướng và chuyển tiếp của URL

Lỗ hổng 10: Sử dụng các lỗ hổng có sẵn trong thư viện

1.4. Các phương thức tấn công website phổ biến

1.4.1. Giới thiệu chung

1.4.2. Các phương thức tấn công website

1.4.2.1. Tấn công SQL injection

1.4.2.2. Tấn công kiểu Broken Authentication And Session Management

1.4.2.3. Tấn công XSS

1.4.2.4. Tấn công Insecure Direct Object References

1.4.2.5. Tấn công Security Misconfiguration

1.4.2.6. Tấn công Sensitive Data Exposure

1.4.2.7. Tấn công Missing Function Level Access Control

1.4.2.8. Tấn công CSRF

1.4.2.9. Tấn công Using Components with Known Vulnerabilities

1.4.2.10. Tấn công Unvalidated Redirects and Forwards

1.4.2.11. Tấn công DoS, DDoS

1.4.2.12. Tấn công APT

1.5. Kết luận Chương 1

Trong Chương 1, luận văn đã khảo sát, phân loại website dựa trên nhiều tiêu chí, đặc biệt là tiêu chí về mức độ bảo mật. Căn cứ vào thực trạng tấn công website tại Việt Nam và trên thế giới trong những năm gần đây, luận văn đã trình bày các lỗ hổng bảo mật phổ biến của ứng dụng web, các phương thức tấn công website thường gặp và nguy cơ mất an toàn thông tin website của các doanh nghiệp. Từ đó nói lên nhu cầu cấp thiết của việc đảm bảo an toàn thông tin cho website.

Chương tiếp theo, luận văn sẽ nghiên cứu các giải pháp đảm bảo an toàn thông tin cho website.

CHƯƠNG 2. CÁC GIẢI PHÁP ĐẢM BẢO AN TOÀN THÔNG TIN WEBSITE

Trong Chương 2 luận văn sẽ nghiên cứu một số giải pháp đảm bảo an toàn thông tin cho website, cụ thể bao gồm các nội dung sau: triển khai hệ thống phòng thủ, thiết lập và cấu hình hệ thống máy chủ an toàn, vận hành an toàn và phòng chống tấn công từ chối dịch vụ.

2.1. Triển khai hệ thống phòng thủ

2.1.1. Tổ chức mô hình mạng

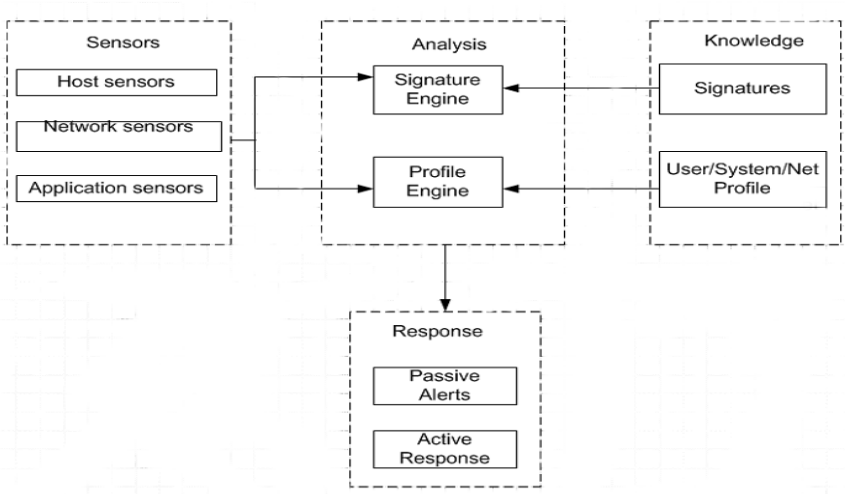
2.1.2. Thiết lập tường lửa

2.1.3. Sử dụng công cụ phát hiện và ngăn chặn xâm nhập (IDS/IPS)

2.1.3.1. Hệ thống phát hiện xâm nhập IDS

Các thành phần của IDS

Các thành phần của hệ thống IDS được mô tả trong [Hình 2.3].



Hình 2.1. Các thành phần của hệ thống IDS

Hệ thống IDS bao gồm các thành phần: Thành phần thu gói tin (Sensors); Thành phần phân tích gói tin (Analysis); Thành phần tri thức (Knowledge) hỗ trợ quá trình phân tích gói tin và Thành phần phản hồi (Respontion) xuất các thông tin cảnh báo.

Snort

Một trong những phần mềm IDS phổ biến hiện nay là Snort. Đây là một sản phẩm NIDS mã nguồn mở với hệ thống signature database (gọi là rule database) được cập nhật thường xuyên bởi nhiều thành viên trong cộng đồng Internet.

2.1.3.2. Hệ thống ngăn chặn xâm nhập IPS

Hệ thống phòng chống xâm nhập (IPS) là một kỹ thuật, kết hợp các ưu điểm của kỹ thuật tường lửa với hệ thống phát hiện xâm nhập IDS, có khả năng phát hiện các cuộc tấn công và tự động ngăn chặn các cuộc tấn công nhằm vào điểm yếu của hệ thống.

Các kiểu triển khai IPS:

- **Out-of-band IPS (OOB IPS)**:
- **In-line IPS**:

2.1.3.3. Ứng dụng hệ thống IDS/IPS chống tấn công web

2.1.4. Ứng dụng phòng chống vi-rút và bảo vệ máy tính cá nhân

2.2. Thiết lập và cấu hình hệ thống máy chủ an toàn

2.2.1. Thiết lập và cấu hình hệ điều hành máy chủ

2.2.2. Thiết lập và cấu hình máy chủ ứng dụng web

2.2.3. Thiết lập và cấu hình máy chủ cơ sở dữ liệu

2.3. Vận hành an toàn

2.3.1. Kiểm tra hoạt động ứng dụng web an toàn

2.3.2. Một số biện pháp ứng phó với tấn công

2.3.3. Đào tạo đội ngũ nhân lực vận hành hệ thống

2.4. Tấn công từ chối dịch vụ và cách phòng chống

2.4.1. Tấn công từ chối dịch vụ (DoS)

2.4.2. Tấn công từ chối dịch vụ phân tán (DDoS)

2.4.3. Tấn công từ chối dịch vụ phản xạ nhiều vùng (DRDoS)

2.4.4. Phân loại tấn công DDoS

Một số loại tấn công DDoS nổi bật như sau:

SYN Flood:

UDP Flood:

HTTP Flood:

Ping of Death:

Smurf Attack:

Fraggle Attack:

Slowloris:

Application Level Attacks:

NTP Amplification:

Advanced Persistent DoS (APDoS):

Zero-day DDoS Attacks:

2.4.5. Phòng chống tấn công từ chối dịch vụ

2.5. Đề xuất ứng dụng các giải pháp đảm bảo an toàn thông tin website đối với các doanh nghiệp vừa và nhỏ

2.5.1. Phương án tổ chức mô hình mạng cho hệ thống máy chủ web

Xây dựng mô hình mạng bao gồm cụm máy chủ ứng dụng web, máy chủ chứa dữ liệu ảnh CDN và cụm máy chủ chứa cơ sở dữ liệu.

Máy chủ ứng dụng web và máy chủ chứa dữ liệu ảnh cần được đặt trên vùng mạng DMZ. Máy chủ ứng dụng web được cài đặt mã nguồn website PHP và điều hướng cũng như xử lý truy cập bằng dịch vụ Nginx.

Máy chủ ứng dụng web chỉ mở kết nối từ domain và có thể truy cập đến máy chủ CDN ở cùng vùng mạng DMZ để lấy dữ liệu ảnh. Dữ liệu web được lấy từ cơ sở dữ liệu thông qua việc truy cập đến cơ sở dữ liệu tại vùng mạng nội bộ.

Máy chủ chứa cơ sở dữ liệu được đặt ở vùng mạng nội bộ của doanh nghiệp, được cài đặt hệ quản trị cơ sở dữ liệu (MySql). Máy chủ này chỉ mở cổng truy cập trực tiếp từ IP của vùng mạng DMZ - máy chủ ứng dụng web.

Việc tổ chức mô hình mạng máy chủ như vậy giúp cho website của doanh nghiệp có thể tránh được những tấn công trực tiếp đến IP của máy chủ web và máy chủ cơ sở dữ liệu từ môi trường Internet.

2.5.2. Thiết lập tường lửa cho máy chủ web

Máy chủ ứng dụng web nên sử dụng VPS hệ điều hành Centos được cài đặt dịch vụ tường lửa Iptables. Với dịch Iptables ta có thể thiết lập để mở và đóng truy cập từ các IP và

cổng khác nhau. Cụ thể ta chỉ cho phép truy cập máy chủ web thông qua truy cập vào website bằng cổng 80 và 443 tương ứng với giao thức http và https.

Sử dụng cấu hình trong Iptables chỉ cho phép truy cập đến máy chủ thông qua 2 cổng trên. Mặc định những truy cập từ cổng khác sẽ bị chặn như SSH, FTP, SMTP…

```
# iptables -I INPUT -p tcp -m tcp --dport 80 -j ACCEPT
# iptables -I INPUT -p tcp -m tcp --dport 443 -j ACCEPT
```

2.5.3. Cấu hình máy chủ web và máy chủ cơ sở dữ liệu

Máy chủ web của doanh nghiệp được đặt ở vùng mạng DMZ với 2 cụm là cụm máy chủ ứng dụng được cài đặt mã nguồn website và máy chủ CDN chứa dữ liệu ảnh của web. Trong đó, máy chủ ứng dụng web sử dụng điều hướng bằng dịch vụ Nginx, để quản lý truy cập đến website cũng như tài nguyên.

Dịch vụ điều hướng Nginx được cấu hình để chỉ mạng nội bộ mới truy cập được mô đun quản trị và duyệt thư mục tài nguyên của website. Còn lại những truy cập của khách vãng lai sẽ chỉ xem được mô đun giao diện người dùng. Như vậy chỉ những người có quyền quản trị website và sử dụng mạng nội bộ của doanh nghiệp mới được phép truy cập vào mô đun quản trị cũng như duyệt thư mục chứa tài nguyên của website.

Bên cạnh đó máy chủ web cần được cài đặt để lưu thông tin truy cập của tất cả khách thông qua dịch vụ lưu nhật ký của mã nguồn. Điều này cho phép quản trị viên kiểm tra được những truy cập bất thường hoặc những truy cập gặp lỗi trên website.

Máy chủ chứa cơ sở dữ liệu của website được đặt ở môi trường mạng nội bộ, chỉ cho phép truy cập từ IP của máy chủ ứng dụng web với cổng 3306 của hệ điều hành MySql.

2.5.4. Vận hành website

Để vận hành website ổn định và đảm bảo tính bảo mật thông tin, doanh nghiệp cần xây dựng một đội ngũ nhân viên IT và quy trình vận hành chuyên nghiệp.

Đội ngũ IT có nhiệm vụ nâng cấp hệ thống website bao gồm mã nguồn theo yêu cầu tính năng và phần cứng đáp ứng website hoạt động bình thường. Đồng thời vận hành website, thường xuyên kiểm tra những truy cập thông qua hệ thống Logging (nhật ký), tìm ra và giải quyết những vấn đề xảy ra hàng ngày như lỗi web hoặc có tấn công từ tin tặc.

Quyền quản trị trên website phải được phân chia rõ ràng, tài khoản riêng được cấp cho mỗi cá nhân để đảm bảo những hành động trên mô đun quản trị đều được ghi lại và gán trách nhiệm cho từng người.

Dữ liệu của website bao gồm dữ liệu ảnh, văn bản và dữ liệu trong cơ sở dữ liệu cần được quản trị viên thường xuyên backup để đảm bảo khi có sự cố xảy ra, có thể khôi phục lại bình thường một cách nhanh chóng, tránh mất dữ liệu quan trọng của hệ thống.

2.6. Kết luận Chương 2

Trong Chương 2, luận văn đã khảo sát 04 nhóm giải pháp đảm bảo thông tin cho website, bao gồm: triển khai hệ thống phòng thủ, thiết lập và cấu hình hệ thống máy chủ an toàn, vận hành an toàn và phòng chống tấn công từ chối dịch vụ. Trong đó, tập trung vào các giải pháp phòng chống tấn công từ chối dịch vụ. Từ đó phân tích ứng dụng thực tế các giải pháp cho việc đảm bảo an toàn Website của doanh nghiệp vừa và nhỏ, đảm bảo chi phí hợp lý và mức độ an toàn cần thiết.

Trên cơ sở đó, trong chương tiếp theo, luận văn sẽ tiến hành đánh giá mức độ bảo mật website của Sở Thông tin và Truyền thông Hà Nội và đưa ra các giải pháp nâng cao mức độ bảo mật.

CHƯƠNG 3. ĐÁNH GIÁ MỨC ĐỘ BẢO MẬT WEBSITE CỦA SỞ THÔNG TIN VÀ TRUYỀN THÔNG HÀ NỘI

Trong Chương 3 luận văn tiến hành đánh giá mức độ bảo mật website Sở Thông tin và Truyền thông Hà Nội và đưa ra các giải pháp nâng cao bảo mật.

3.1. Đặc điểm website của doanh nghiệp vừa và nhỏ

*** Về chức năng**

*** Về mức độ bảo mật**

*** Về hệ thống**

3.2. Tiêu chí đánh giá độ bảo mật website của doanh nghiệp vừa và nhỏ

*** Khả năng ngăn chặn spam**

*** Khả năng chống tấn công DDoS**

*** Khả năng chống tấn công Brute Force**

*** Khả năng chống tấn công XSS**

*** Khả năng chống tấn công SQL injection**

*** Trang web có chứng chỉ SSL hay không?**

*** Trang web có sử dụng HTTP/2 hay không?**

*** Khả năng chống tấn công lỗi chứng thực yếu (Insufficient Authentication)**

*** Khả năng chống tấn công liệt kê thư mục (Directory Indexing)**

*** Khả năng chống tấn công lỗ hổng tải lên tệp tin thực thi.**

*** Khả năng sao lưu dữ liệu**

3.3. Đánh giá mức độ bảo mật website của Sở Thông tin và Truyền thông Hà Nội

3.3.1. Sở Thông tin và Truyền thông Hà Nội và hệ thống website

Sở Thông tin và Truyền thông thành phố Hà Nội (sau đây gọi tắt là Sở) là cơ quan chuyên môn thuộc Ủy ban nhân dân Thành phố có chức năng tham mưu, giúp Ủy ban nhân dân Thành phố quản lý nhà nước về: báo chí; xuất bản; bưu chính; viễn thông; tần số vô tuyến điện; công nghệ thông tin; điện tử; phát thanh và truyền hình; thông tin đối ngoại; bản tin thông tấn; thông tin cơ sở; hạ tầng thông tin truyền thông; quảng cáo trên báo chí, trên môi trường mạng, trên xuất bản phẩm và quảng cáo tích hợp trên các sản phẩm, dịch vụ bưu chính, viên thông, công nghệ thông tin.

Sở chịu sự chỉ đạo, quản lý về tổ chức, biên chế và công tác của Ủy ban nhân dân Thành phố, đồng thời chịu sự chỉ đạo, kiểm tra, hướng dẫn về chuyên môn, nghiệp vụ của Bộ Thông tin và Truyền thông.

Là Sở ngành dẫn đầu toàn thành phố về mức độ ứng dụng công nghệ thông tin trong hoạt động quản lý nhà nước, Sở đang cung cấp 28 dịch vụ công trực tuyến mức độ 3 trên website của Sở tại địa chỉ https://sotttt.hanoi.gov.vn/, và tích hợp trên cổng dịch vụ công quốc gia. Ngoài ra, website của Sở có đặt đường dẫn trực tiếp đến cổng dịch vụ công của thành phố Hà Nội với tổng số 1828 thủ tục hành chính.

Với những đặc điểm website của doanh nghiệp vừa và nhỏ đã nêu ở mục 3.1, có thể nhận thấy một số điểm tương đồng với website của Sở Thông tin và Truyền thông Hà Nội. Cụ thể:

- Về chức năng: website của Sở cung cấp, cập nhật những thông tin về hoạt động của sở, những văn bản chỉ đạo liên quan của Thành phố, những thông tin này đều là thông tin nhạy cảm, nếu bị tin tặc tấn công làm sai lệch sẽ gây ra hậu quả vô cùng nghiêm trọng, đặc biệt trong tình hình diễn biến dịch bệnh Covid-19 phức tạp như hiện nay.

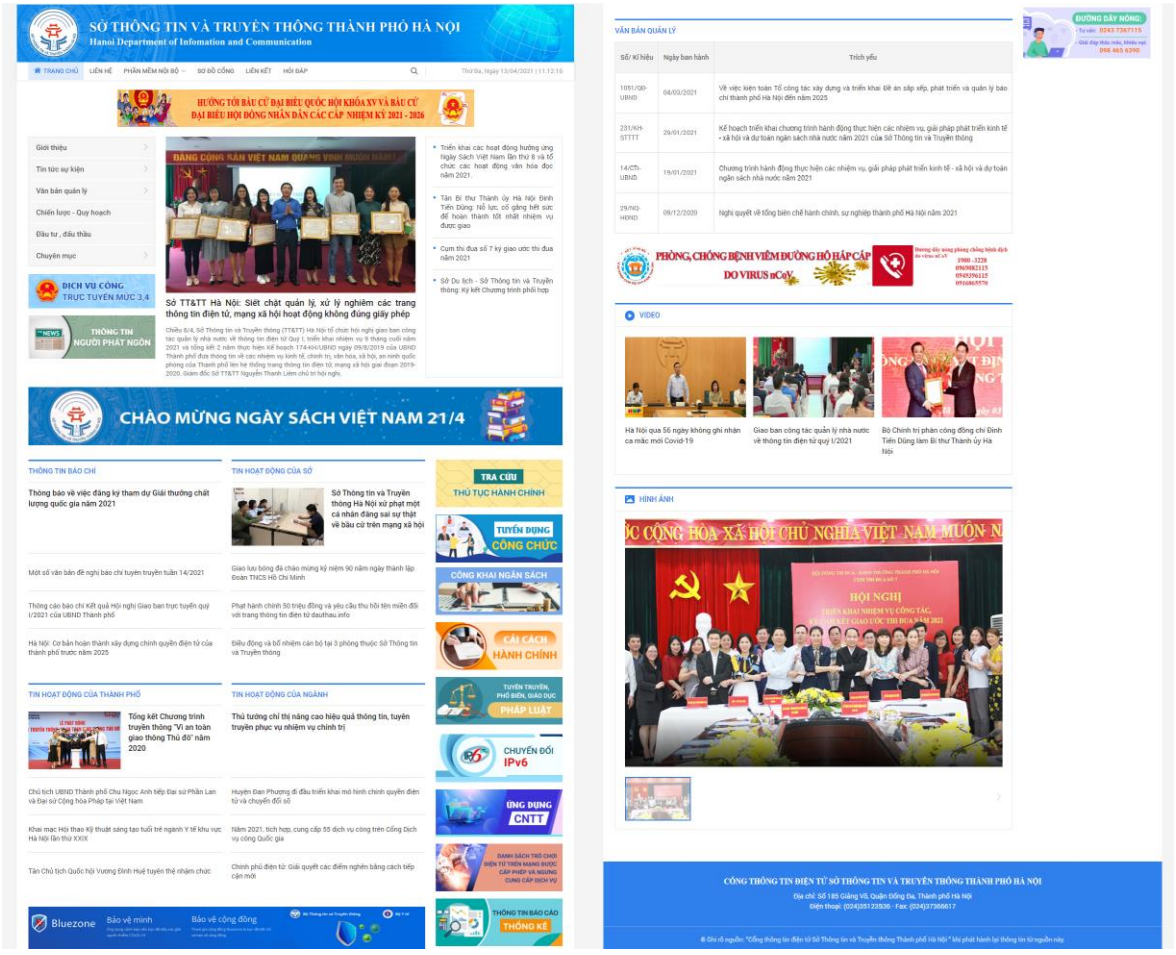
- Về mức độ bảo mật: website của doanh nghiệp vừa và nhỏ và website của Sở đều yêu cầu độ bảo mật cao do chứa đựng những thông tin nhạy cảm, quan trọng.

- Về hệ thống: Mặc dù website của Sở yêu cầu độ bảo mật cao nhưng hiện tại vẫn chưa được quan tâm đúng mực, chưa có đội ngũ quản trị riêng mà chỉ có một số ít nhân sự đảm nhận nhiệm vụ làm nội dung, thực hiện đăng tải những thông tin, văn bản đã được lãnh đạo phê duyệt.

Nhận thấy những điểm tương đồng nêu trên, học viên đã lựa chọn đánh giá mức độ bảo mật website của Sở để phù hợp với yêu cầu của đề tài nhưng vẫn có ý nghĩa thực tiễn, phục vụ cho công việc quản lý nhà nước của học viên tại Sở Thông tin và Truyền thông Hà Nội. [Hình 3.2] mô tả giao diện trang chủ của website của Sở Thông tin và Truyền thông Hà Nội.

3.3.2. Đánh giá mức độ bảo mật website của Sở Thông tin và Truyền thông Hà Nội

Về mặt giải pháp đảm bảo an toàn thông tin website, thì website của Sở Thông tin và Truyền thông Hà Nội cơ bản đã tuân theo các đề xuất như trong mục 2.5 (Trình bày ở Chương 2).



Hình 3.1. Giao diện trang chủ website Sở Thông tin và Truyền thông Hà Nội

Cùng với những tiêu chí đã nêu ở mục 3.1, học viên tiến hành đánh giá mức độ bảo mật website của Sở Thông tin và Truyền thông Hà Nội. Cụ thể như sau:

*** Khả năng ngăn chặn spam**

Website của Sở hiện chỉ cung cấp một form cho phép người dùng nhập câu hỏi, góp ý ở địa chỉ : https://sotttt.hanoi.gov.vn/dat-cau-hoi.htm

Nội dung biểu mẫu nhập được kiểm tra các kiểu dữ liệu tương ứng, đồng thời khi gửi biểu mẫu cần phải điền mã captcha tự động sinh sau mỗi truy cập, nếu captcha không khớp sẽ không thể gửi biểu mẫu thông tin. Nội dung gửi lên hệ thống đều phải qua kiểm duyệt chứ không hiển thị lên danh sách câu hỏi trên giao diện trang web.

Đánh giá: Website đã có cơ chế chặn spam nội dung rác trong các biểu mẫu nhập thông tin người dùng.

*** Khả năng chống tấn công DDoS**

Máy chủ của website hiện đang dùng Nginx để phân tải cũng như điều hướng truy cập. Với Nginx có thể thực hiện được một số tác vụ nhằm hạn chế tấn công DDoS như :

Giới hạn tần suất gửi các truy cập từ một địa chỉ IP

Giới hạn số lượng truy cập từ 1 IP đến một địa chỉ bất kỳ trên website

Chặn một số IP nghi ngờ

Giới hạn số lượng kết nối đến máy chủ, nếu vượt quá số lượng truy cập sẽ từ chối yêu cầu.

Đánh giá : Website đã triển khai phân tải bằng Nginx, tránh được một phần rủi ro bị tấn công DDoS.

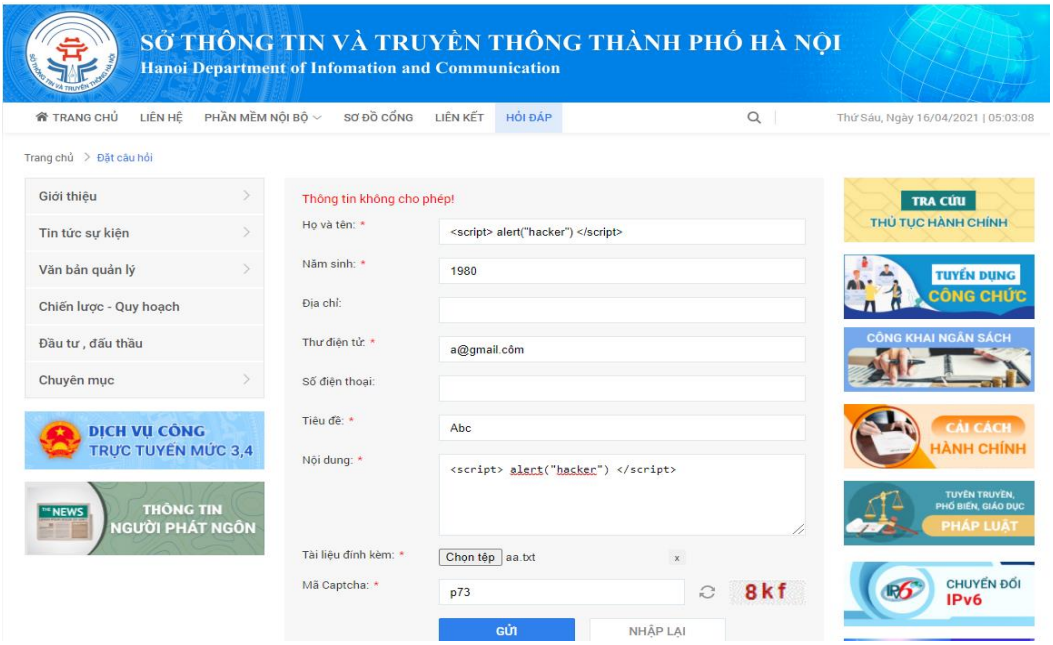
*** Khả năng chống tấn công Brute Force**

Website của Sở không cho phép khách vãng lai đăng ký hay đăng nhập trên hệ thống. Đồng thời trang quản trị CMS cũng không công khai trên mạng internet, chỉ có thể truy vấn bằng mạng nội bộ.

Đánh giá : Website không có rủi ro bị tấn công BruteForce.

*** Khả năng chống tấn công XSS**

Tiến hành thử nhúng mã script vào biểu mẫu nhập thông tin của website là phần đặt câu hỏi. Hệ thống đã chặn không cho phép gửi các thông tin chứa đoạn mã thực thi.



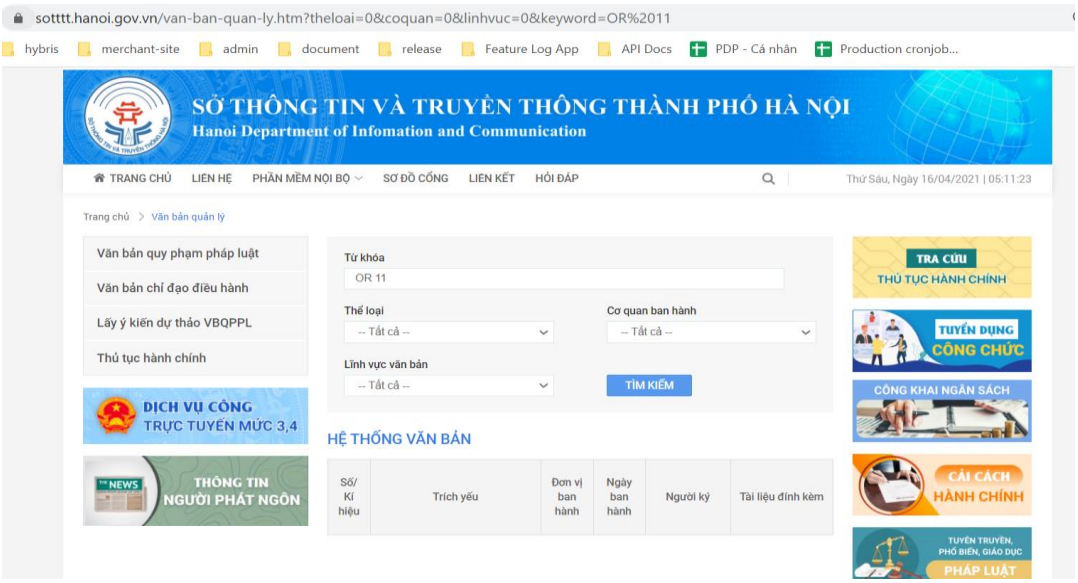
Đánh giá: Website có khả năng chống tấn công XSS

*** Khả năng chống tấn công SQL Injection**

Tại trang tìm kiếm văn bản trên website : https://sotttt.hanoi.gov.vn/van-ban-quan-ly.htm

Thực hiện nhập thông tin tìm kiếm vào trường Từ Khóa với nội dung nhằm tấn công SQL Injection : 'OR 1=1'

Hệ thống tự động xóa những ký tự đặc biệt = và ''



Đánh giá : Website đã có cơ chế ngăn chặn tấn công SQL Injection.

*** Chứng chỉ SSL**

Hiện tại website https://sotttt.hanoi.gov.vn/ đã có chứng chỉ SSL, nếu truy cập bằng giao thức http, hệ thống tự động chuyển hướng sang giao thức https thông qua Nginx.

*** Giao thức Http/2.0**

Dùng công cụ kiểm tra trang web có hỗ trợ http/2.0 cho trang web, kết quả hiện tại website đã hỗ trợ giao thức http/2.0

*** Khả năng chống tấn công dựa vào lỗi chứng thực yếu**

Thực hiện truy vấn vào địa chỉ bảo mật bằng quyền quản trị mà không có quyền này. Hệ thống báo lỗi 403 - Forbidden, như vậy website đã tránh được nguy cơ tấn công lỗi chứng thực yếu.

*** Khả năng chống tấn công liệt kê thư mục**

Thực hiện cố tình truy vấn vào tên miền chứa dữ liệu ảnh của website: https://sotttt.qltns.mediacdn.vn/

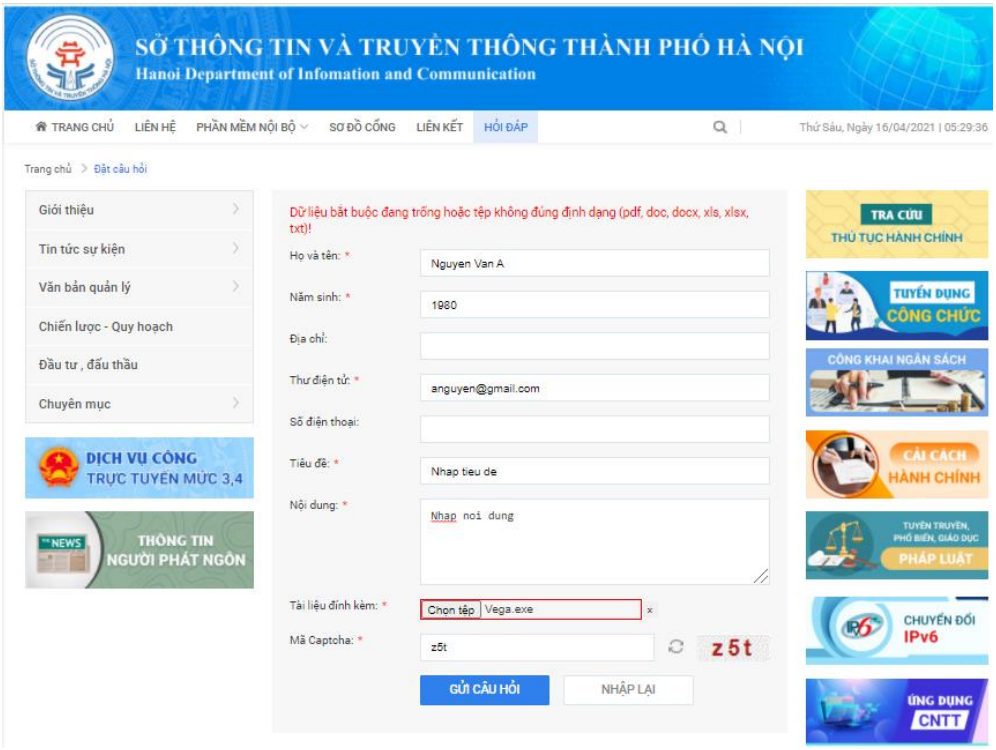
Hệ thống báo URL không tồn tại, như vậy không thể truy cập các thư mục chứa dữ liệu của website thông qua tấn công liệt kê thư mục.

*** Nguy cơ tấn công tải lên tập tin thực thi**

Hiện website có duy nhất một form cho phép tải tập tin lên hệ thống là mục đặt câu hỏi cho sở thông tin, tại địa chỉ : https://sotttt.hanoi.gov.vn/dat-cau-hoi.htm

Tại đây, hệ thống chỉ cho phép tải lên những tập tin dữ liệu định dạng văn bản bao gồm : pdf, doc, docx, xls, xlsx, txt

Thực hiện tải tập tin với định dạng thực thi là .exe, hệ thống báo lỗi không được phép tải lên.



Nhưng khi thực hiện đổi định dạng của tập tin thực thi từ .exe sang .txt (bản chất vẫn là tập tin thực thi của hệ điều hành window). Lúc này thực hiện tải lên, hệ thống vẫn cho tải lên thành công.

Đánh giá: Đây là lỗi khá nghiêm trọng, khi hệ thống chưa phát hiện được nội dung file có đúng theo yêu cầu hay không.

*** Sao lưu dữ liệu website**

Hiện nay website của Sở đang có các CronJob tự động sao lưu dữ liệu website theo lịch cố định.

3.4. Đề xuất một số giải pháp nâng cao bảo mật

3.4.1. Sử dụng CloudFlare chống DDoS cho website

Hiện tại website của Sở chưa có cơ chế mạnh mẽ chống tấn công DDoS. Do đó có thể bổ sung một phương pháp hiệu quả hơn thay vì chỉ sử dụng phân tải bằng Nginx.

Một trong những cơ chế hiệu quả và đang được sử dụng thịnh hành đó là CloudFlare. Trước tiên CloudFlare là một dịch vụ CDN & DDNS kết hợp để gia tăng tốc độ & tính bảo mật cho website. Khi website sử dụng CloudFlare, mọi truy xuất đến website đó sẽ được định tuyến qua hệ thống thông minh của CloudFlare.

Trường hợp sử dụng CloudFlare thì mọi truy vấn đến website sẽ không còn là truy vấn trực tiếp nữa mà phải đi qua CloudFlare. Và chỉ những truy cập tin cậy mới có thể thông qua CloudFlare để đi đến website. Các truy vấn bị nghi ngờ như tấn công hệ thống của các tin tặc, spam bot, tấn công DDoS… sẽ bị ngăn chặn và loại bỏ.

Đồng thời website cũng được CloudFlare che dấu địa chỉ IP máy chủ web, cũng tránh được rủi ro tấn công DDoS.

Để sử dụng CloudFlare cho website, cần phải đăng ký tài khoản CloudFlare tại địa chỉ : https://dash.cloudflare.com/sign-up

Sau đó tiến hành thay đổi DNS hiện tại thành DNS của Cloudflare. Tất cả cấu hình chỉ cần thực hiện trên hệ thống CloudFlare, đều có hướng dẫn chi tiết đến từ nhà cung cấp.

3.4.2. Chống tấn công tải lên tập tin thực thi

Như tiêu chí đánh giá bảo mật - tấn công tải lên tập tin thực thi, website của Sở Thông tin và Truyền thông Hà Nội vẫn gặp lỗi có thể tải lên hệ thống tập tin có định dạng văn bản nhưng thực chất là tập tin thực thi (chỉ cần đổi tên mở rộng của của tập tin).

Để ngăn chặn tải lên tập tin không đúng định dạng trong ngông ngữ lập trình PHP, ta cần thêm hàm kiểm tra dựa theo MimeType của tập tin. Cụ thể ta cần kiểm tra xem tập tin lên có đúng định dạng txt, doc, docs, pdf, xls, xlsx:

Tương ứng các MimeType sau :

text/plain

application/msword

application/vnd.openxmlformats officedocument.wordprocessingml.document

application/pdf

application/vnd.ms-excel

application/vnd.openxmlformats-officedocument.spreadsheetml.sheet

Function kiểm tra MimeType của tập tin :

```
<?php
$mimetype = mime_content_type($_FILES['file']['tmp_name']);
if(in_array($mimetype, array(application/msword ', ' application/vnd.openxmlformats officedocument.wordprocessingml.document', ' application/pdf',' text/plain',' application/vnd.ms-excel',' application/vnd.openxmlformats-officedocument.spreadsheetml.sheet'))) {
    uploadFile();
    echo 'OK';

} else {
   echo 'Không đúng định dạng file!';
}
```

Như vậy với hàm kiểm tra này ta đã chặn được việc tải lên các tập tin dữ liệu với tên mở rộng là tập tin văn bản nhưng bản chất là các tập tin thực thi.

3.5. Kết luận Chương 3

Trong Chương 3, luận văn đã giới thiệu sơ lược về Sở Thông tin và Truyền thông Hà Nội và hệ thống website; khảo sát và đưa ra bộ tiêu chí đánh giá mức độ bảo mật website nói chung, thực hiện đánh giá thực tế mức độ bảo mật website của Sở. Từ đó đề xuất một số giải pháp để nâng cao tính bảo mật và độ an toàn đối với website của Sở.

KẾT LUẬN

Trước tình hình an ninh mạng ngày càng trở nên nóng bỏng với hàng loạt vụ tấn công nhắm vào website của các cơ quan nhà nước và doanh nghiệp, đặc biệt là các doanh nghiệp vừa và nhỏ với số lượng tăng lên theo từng năm và mức độ ngày càng tinh vi, phức tạp. Nhận ra tính cấp thiết, ý nghĩa khoa học và thực tiễn của vấn đề nghiên cứu các giải pháp bảo mật cho website, học viên đã chọn đề tài **"Nghiên cứu giải pháp bảo mật website cho các doanh nghiệp vừa và nhỏ"** cho luận văn tốt nghiệp trình độ đào tạo thạc sĩ, phù hợp với đặc thù công việc quản lý nhà nước tại Sở Thông tin và Truyền thông Hà Nội, nơi học viên đang công tác.

Học viên đã tìm tòi, nghiên cứu, tổng hợp thông tin từ nhiều nguồn tài liệu trong và ngoài nước, các diễn đàn về bảo mật thông tin, cũng như kinh nghiệm quản lý về an ninh thông tin của học viên để thực hiện các nội dung của luận văn. Mặc dù những nội dung về lý thuyết mà học viên tổng hợp được không phải là mới, nhưng nó rất có ý nghĩa đối với học viên, qua đó học viên đã được học hỏi, trau dồi kiến thức cho bản thân, tạo tiền đề giúp cho học viên thực hiện những mục tiêu cao hơn trong tương lai. Cùng với sự hướng dẫn tận tình của thầy giáo hướng dẫn, luận văn đã đạt được một số kết quả sau đây:

- Khảo sát thực trạng bảo mật website tại Việt Nam và trên thế giới, nghiên cứu tổng quan về bảo mật website, các tiêu chí phân loại website. Từ những kiến thức tổng hợp được, đưa ra tiêu chí mới để phân loại website, đó là ***phân loại website dựa trên mức độ bảo mật.***

- Nghiên cứu 04 nhóm giải pháp đảm bảo an toàn thông tin cho website, bao gồm: triển khai hệ thống phòng thủ, thiết lập và cấu hình hệ thống máy chủ an toàn, vận hành an toàn và phòng chống tấn công từ chối dịch vụ. Trong đó, tập trung đi sâu vào các giải pháp phòng chống tấn công từ chối dịch vụ. Đề xuất ứng dụng các giải pháp để đảm bảo anh toàn thông tin website cho các doanh nghiệp vừa và nhỏ phù hợp với thực tế, đảm bảo an toàn và tiết kiệm kinh phí.

- Giới thiệu sơ lược về Sở Thông tin và Truyền thông Hà Nội và hệ thống website, khảo sát và tổng hợp ra bộ tiêu chí đánh giá mức độ bảo mật website nói chung, thực hiện đánh giá thực tế mức độ bảo mật website của Sở Thông tin và Truyền thông Hà Nội. Từ đó đề xuất một số giải pháp để nâng cao tính bảo mật và độ an toàn đối với website của Sở.

Qua các kết quả đánh giá ban đầu cho thấy, website Sở Thông tin và Truyền thông Hà Nội có độ bảo mật khá cao, có thể tránh được những rủi ro tấn công cơ bản nhất từ tin tặc như: có khả năng chặn spam, chống tấn công Brute Force, XSS, SQL Injection, chống tấn công liệt kê thư mục, lỗi chứng thực yếu... Bên cạnh đó vẫn còn tồn tại những hạn chế như khả năng chống tấn công DDoS và chống tấn công tải lên tập tin thực thi chưa cao.

Để nâng cao tính bảo mật và độ an toàn website của Sở Thông tin và Truyền thông Hà Nội, khắc phục những tồn tại nêu trên, học viên đã đề xuất thực hiện 02 giải pháp. Trong đó, giải pháp sử dụng CloudFlare để chống tấn công DDoS cho website và giải pháp bổ sung thêm hàm kiểm tra trong ngôn ngữ lập trình PHP dựa theo MimeType của tập tin để kiểm tra chính xác định dạng của tệp tin, ngăn chặn việc tải lên tệp tin thực thi.

Trong thời gian tới, học viên sẽ làm việc với đội ngũ quản trị website của Sở Thông tin và Truyền thông Hà Nội để đề xuất thực hiện các giải pháp nâng cao tính bảo mật nêu trên. Đồng thời, bản thân học viên sẽ tiếp tục nghiên cứu sâu hơn lĩnh vực an toàn thông tin nói chung và bảo mật website nói riêng, nhằm phục vụ cho những nhiệm vụ khác của Sở Thông tin và Truyền thông Hà Nội và cho công việc kiểm tra, rà soát, xử lý vi phạm trên môi trường mạng mà học viên đang phụ trách.