BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 2132/BTTTT-VNCERT

V/v Hướng dẫn đảm bảo an toàn thông tin cho các Cổng/Trang thông tin điện tử

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc Lập - Tự Do - Hạnh Phúc

Hà Nội, ngày 18 tháng 7 năm 2011

BỘ KHOA HỌC & CÔNG NGHỆ
TRUNG TÂM TIN HỌC
CÔNG VĂN ĐẾN
Số: 3327
Ngày 4 tháng 8 năm 11

Kính gửi:
- Các Bộ, cơ quan ngang Bộ, cơ quan trực thuộc Chính phủ;
- UBND các tỉnh, thành phố trực thuộc Trung ương.

Thực hiện chỉ đạo của Thủ tướng Chính phủ về việc đảm bảo an toàn thông tin cho các cổng thông tin điện tử, đồng thời để thống nhất về nội dung và phương pháp quản lý an toàn thông tin theo yêu cầu của Nghị định của Chính phủ số 43/2011/NĐ-CP ngày 13/6/2011, Bộ Thông tin và Truyền thông hướng dẫn các cơ quan nhà nước triển khai áp dụng tài liệu "Hướng dẫn một số biện pháp kỹ thuật cơ bản đảm bảo an toàn cho cổng/trang thông tin điện tử". Tài liệu này bao gồm một số biện pháp kỹ thuật thiết yếu nhất nhằm đảm bảo xây dựng và vận hành an toàn các cổng/trang thông tin điện tử và được trình bày trong văn bản gửi kèm theo công văn này.

Trong quá trình triển khai thực hiện, mọi góp ý và đề xuất xin đề nghị Quý cơ quan phản ánh về Bộ Thông tin và Truyền thông, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT).

Xin trân trọng cám ơn./.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Nguyễn Minh Hồng

Nơi nhận:
- Như trên;
- Phó TTg CP Nguyễn Thiện Nhân (để b/c);
- Bộ TT&TT: Bộ trưởng và các Thứ trưởng, các cơ quan đơn vị thuộc Bộ;
- Văn phòng TW Đảng;
- Văn phòng Quốc hội;
- Văn phòng Chính phủ;
- Cơ quan TW các đoàn thể;
- Toà án nhân dân tối cao;
- Viện kiểm sát nhân dân tối cao;
- Kiểm toán nhà nước;
- Ban chỉ đạo quốc gia về CNTT;
- Ban chỉ đạo CNTT các cơ quan Đảng;
- Đơn vị chuyên trách CNTT các Bộ, cơ quan ngang Bộ, cơ quan chính phủ;
- Sở TT&TT các tỉnh, TP thuộc TW;
- Các tập đoàn kinh tế NN;
- Lưu VT, VNCERT.

HƯỚNG DẪN
MỘT SỐ BIỆN PHÁP KỸ THUẬT CƠ BẢN ĐẢM BẢO AN TOÀN CHO CỔNG/TRANG THÔNG TIN ĐIỆN TỬ

(Kèm theo công văn số 2432/BTTTT-VNCERT ngày 18 /7/2011 của Bộ Thông tin và Truyền thông)

1. PHẠM VI VÀ ĐỐI TƯỢNG ÁP DỤNG

1.1. Phạm vi áp dụng

Tài liệu hướng dẫn này được xây dựng nhằm mục đích cung cấp những kiến thức và chỉ dẫn kỹ thuật cơ bản về việc đảm bảo an toàn thông tin (ATTT) đối với hệ thống phần cứng và phần mềm thuộc cổng/trang thông tin điện tử (TTĐT), các yêu cầu thiết lập hệ thống phòng thủ và bảo vệ, qua đó giúp các đơn vị quản lý cổng/trang TTĐT có thể đánh giá mức độ ATTT và lựa chọn giải pháp phù hợp nhằm xây dựng một cổng/trang TTĐT an toàn.

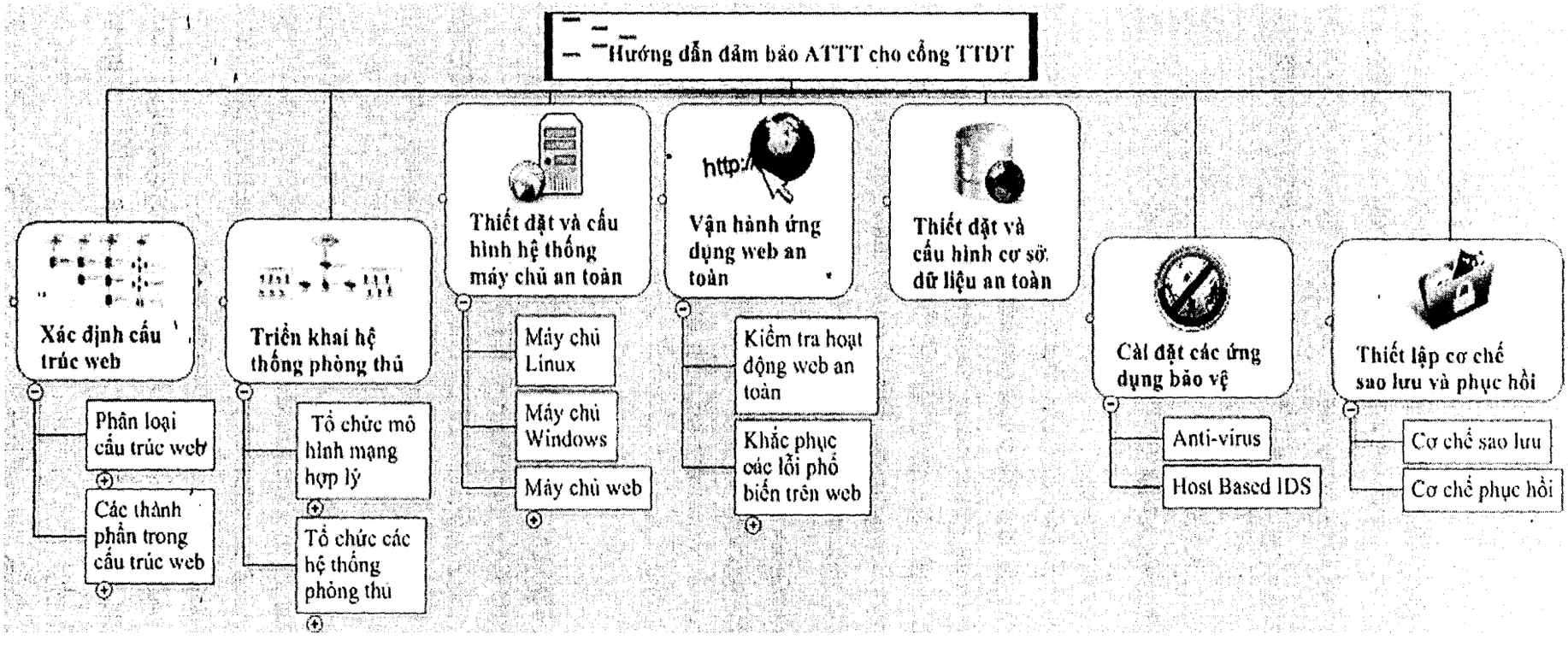
1.2. Đối tượng áp dụng

Các cổng/trang TTĐT của các cơ quan nhà nước và các doanh nghiệp được khuyến cáo tổ chức thực hiện áp dụng tối đa các biện pháp này trong điều kiện cụ thể cho phép.

2. TỔNG QUAN VỀ CÁC BIỆN PHÁP KỸ THUẬT CƠ BẢN ĐẢM BẢO ATTT CHO CỔNG/TRANG TTĐT

Một ứng dụng web nói chung hay cổng/trang TTĐT nói riêng khi triển khai được trên mạng Internet ngoài yếu tố mã nguồn ứng dụng web, còn có những thành phần khác như: máy chủ phục vụ web, hệ quản trị cơ sở dữ liệu,... Do vậy, một cổng/trang TTĐT an toàn đòi hỏi bản thân mã nguồn của cổng phải được lập trình an toàn, tránh các lỗi bảo mật xảy ra trên ứng dụng web và các thành phần bổ trợ như máy chủ phục vụ web và hệ quản trị cơ sở dữ liệu cho ứng dụng đó cũng phải đảm bảo an toàn.

Các biện pháp đảm bảo ATTT cho cổng/trang TTĐT cần được triển khai cho toàn bộ các thành phần của cổng/trang TTĐT, bao gồm các nội dung sau (xem hình 1):



Hình 1. Nội dung đảm bảo ATTT cho cổng/trang TTĐT

- **Xác định cấu trúc web**: giúp người quản trị xác định được mô hình thiết kế web của đơn vị, qua đó có biện pháp tổ chức mô hình web hợp lý, tránh được các khả năng tấn công leo thang đặc quyền.

- **Triển khai hệ thống phòng thủ**: gồm hai nội dung chính là tổ chức mô hình mạng hợp lý và tổ chức các hệ thống phòng thủ, giúp người quản trị có cách nhìn tổng quan về toàn bộ mô hình mạng của cổng/trang TTĐT của mình, qua đó tổ chức mô hình mạng hợp lý cũng như thiết đặt các hệ thống phòng thủ quan trọng như tường lửa (firewall), thiết bị phát hiện/phòng, chống xâm nhập (IDS/IPS), tường lửa mức ứng dụng web (WAF-web application firewall).

- **Thiết đặt và cấu hình hệ thống máy chủ an toàn**: đây là một phần rất quan trọng trong việc đảm bảo vận hành một cổng/trang TTĐT an toàn. Nội dung này giúp người quản trị cấu hình hệ thống máy chủ một cách hợp lý, giảm thiểu khả năng bị tin tặc tấn công vào máy chủ làm ảnh hưởng đến hoạt động của cổng/trang TTĐT.

- **Vận hành ứng dụng web an toàn**: trình bày các nội dung cơ bản cần thực hiện để vận hành một ứng dụng web an toàn. Người quản trị có thể tham khảo phần Phụ lục I "Mười lỗi ATTT phổ biến trên cổng/trang TTĐT" để qua đó nhận diện nguy cơ mắc lỗi của cổng/trang TTĐT tại đơn vị, có biện pháp khắc phục hợp lý hoặc sửa đổi mã nguồn web để loại bỏ các nguy cơ nói trên.

- **Thiết đặt và cấu hình cơ sở dữ liệu an toàn**: đây cũng là một phần rất quan trọng trong việc vận hành một cổng/trang TTĐT. Cơ sở dữ liệu là nơi lưu trữ toàn bộ dữ liệu quan trọng của cổng/trang TTĐT, vì vậy thường bị tin tặc tìm cách tấn công và khai thác. Nội dung này giúp người quản trị hiểu yêu cầu thiết đặt hợp lý cho cơ sở dữ liệu, tránh các lỗi có thể dẫn đến khả năng bị tấn công.

- **Cài đặt các ứng dụng bảo vệ**: ngoài việc khắc phục lỗi cho các thành phần của một cổng/trang TTĐT, nội dung này sẽ trình bày việc cài đặt các ứng dụng bảo vệ như hệ thống chống virus (Anti-Virus) hay hệ thống phát hiện xâm nhập máy tính (Host Based IDS) nhằm bảo vệ cổng/trang TTĐT một cách chủ động và tổng quát.

- **Thiết lập cơ chế sao lưu và phục hồi**: Việc thiết lập cơ chế sao lưu thường xuyên cho hệ thống nhằm giúp lưu lại các tình trạng khi hệ thống hoạt động ổn định. Các bản sao lưu này sẽ được sử dụng trong trường hợp kiểm tra lỗi hệ thống hoặc phục hồi hệ thống ở trạng thái trước khi bị tấn công trong trường hợp lỗi không thể khắc phục hay sửa chữa.

- **Một số biện pháp kỹ thuật chống tấn công từ chối dịch vụ**: đây là nội dung cuối cùng trong tài liệu này nhằm cung cấp định hướng nâng cao năng lực chống tấn công từ chối dịch vụ DoS và DDoS cho các cổng/trang TTĐT.

3. NỘI DUNG CÁC BIỆN PHÁP KỸ THUẬT CƠ BẢN ĐẢM BẢO ATTT

3.1. Xác định cấu trúc của web

Một ứng dụng web khi triển khai, về cơ bản sẽ có 3 lớp như sau: lớp trình diễn, lớp ứng dụng và lớp cơ sở dữ liệu.

Lớp trình diễn (Web Server) là nơi mà máy chủ cài đặt có tác dụng phục vụ các yêu cầu về Web hay nói cách khác, lớp trình diễn là máy chủ phục vụ web (có thể là: IIS Server, Apache HTTP Server, Apache Tomcat Server,...).

Lớp ứng dụng (Web Application) là nơi các kịch bản hay mã nguồn phát triển ra ứng dụng web thực thi (có thể là: ASP.NET, PHP, JSP, Perl, Python,...).

Lớp cơ sở dữ liệu (Database Server) là nơi mà ứng dụng web lưu trữ và thao tác với dữ liệu (thường dựa trên nền các hệ quản trị cơ sở dữ liệu (CSDL) như: Oracle, SQL Server, MySQL,...).

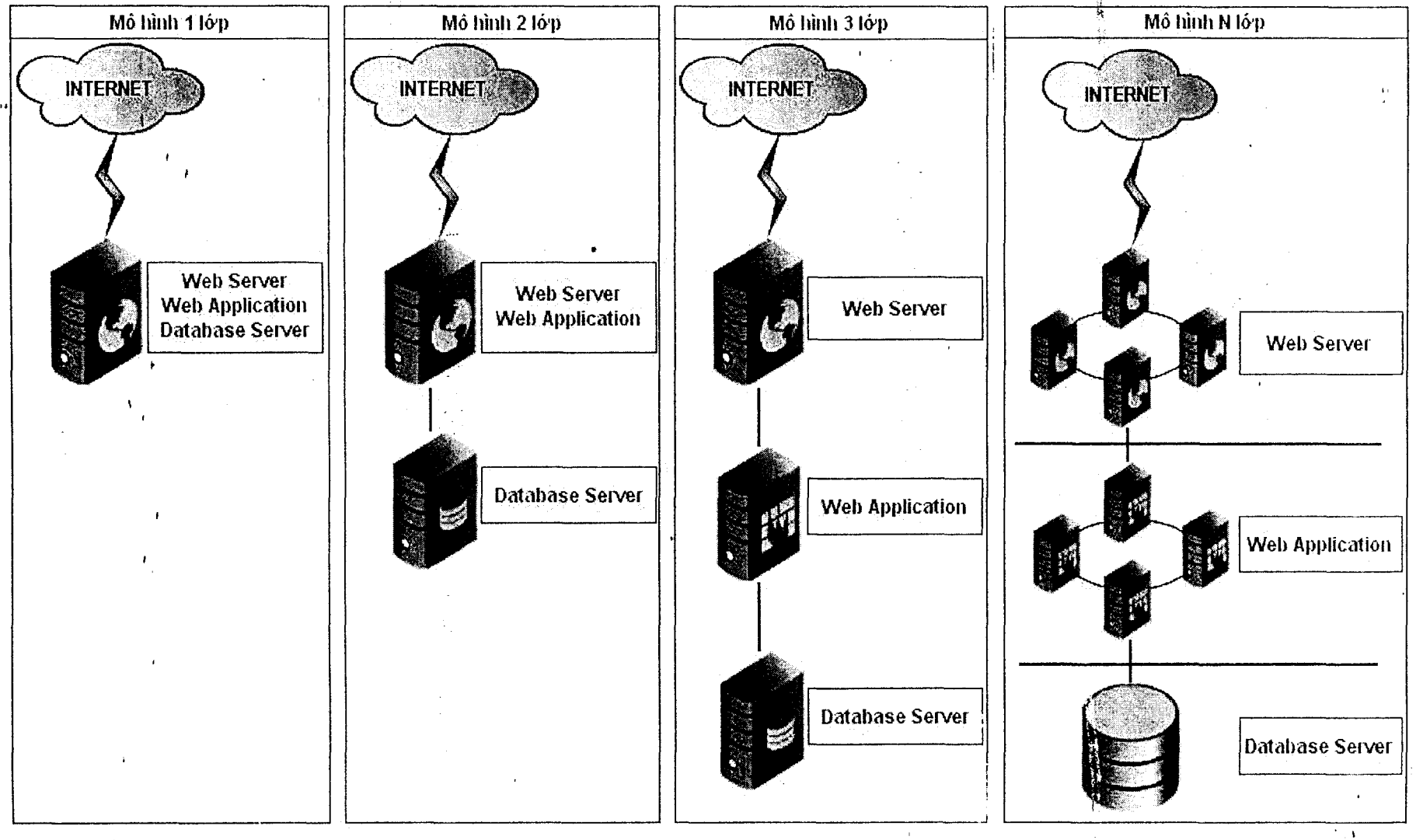
Việc hoạch định tốt các lớp trong cấu trúc web không những giúp người quản trị dễ vận hành mà còn chủ động trong phòng, chống các nguy cơ tấn công từ tin tặc. Một số cách bố trí lớp thường gặp trong thực tế như trên hình vẽ 2.

Mỗi lớp nên khởi tạo một cơ chế phòng thủ riêng cho mình để chống lại những hành động không được phép và không nên "tin tưởng" những lớp khác để tránh tình trạng tấn công leo thang. Một số kịch bản thông dụng:

- Lớp trình diễn có thể áp đặt cơ chế điều khiển truy cập trên một tài nguyên. Ví dụ khi lập chính sách truy cập một tài nguyên nào đó trên hệ thống, chẳng hạn như thư mục */admin*, có thể cài đặt cấu hình lớp trình diễn yêu cầu xác thực với quyền quản trị (administrator). Điều này sẽ hạn chế ảnh hưởng từ lớp ứng dụng có thể sử dụng nhiều kịch bản để truy cập đến tài nguyên trên.

- Lớp cơ sở dữ liệu có thể cung cấp các tài khoản khác nhau với những quyền hành động khác nhau. Ví dụ như với nhóm người sử dụng có tên tài khoản chưa được chứng thực thì thiết đặt quyền thấp nhất là chỉ có thể đọc, còn các thao tác ghi, thay đổi, thực thi là không được phép. Nếu tài khoản được chứng thực thì cũng chỉ được ghi, thay đổi, thực thi trên CSDL đã được chỉ định và chỉ có tác dụng trong phạm vi CSDL đã được cấu hình từ trước.

- Các lớp khác nhau không nên cho phép truy cập đọc hoặc ghi bởi lớp khác. Ví dụ: lớp trình diễn không có khả năng truy cập đến tập tin vật lý được sử dụng lưu trữ dữ liệu tại lớp CSDL mà chỉ có khả năng truy cập dữ liệu này thông qua các truy vấn với các tài khoản phù hợp (truy cập ở cấp độ ứng dụng). Các dịch vụ giao tiếp giữa các lớp trên cấp độ mạng cũng nên được lọc để chỉ cho phép các dịch vụ cần thiết được thực thi. Ví dụ: chỉ cho phép kết nối đến hệ quản trị cơ sở dữ liệu SQL Server trên cổng TCP 1433, còn các cổng khác thì phải được lọc hoặc không cho phép.



Hình 2. Các mô hình triển khai cổng/trang TTĐT

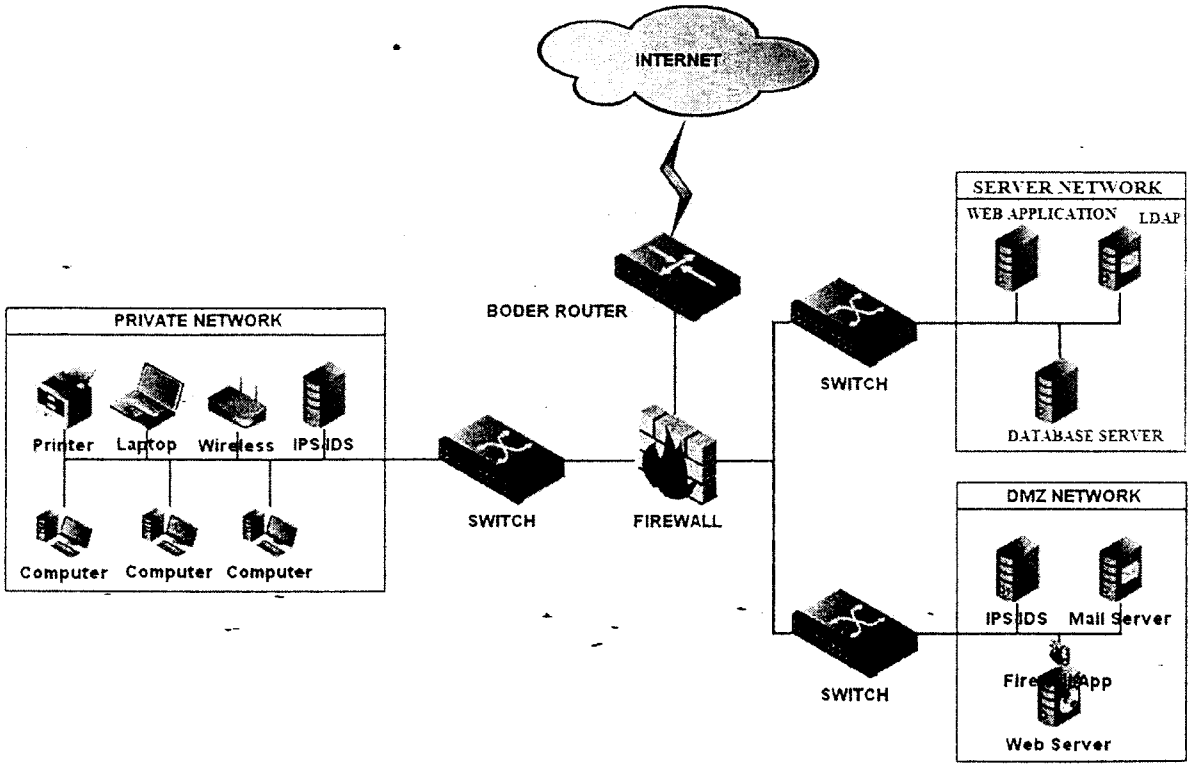
Việc phân tích các mô hình trên cho thấy, nếu giữa các lớp không có sự tách biệt rõ ràng thì khi một lớp bị tin tặc tấn công và chiếm quyền kiểm soát có thể dẫn đến các lớp khác cũng bị ảnh hưởng theo. Ví dụ trường hợp tất cả ứng dụng web, cơ sở dữ liệu đều được đặt trên máy chủ phục vụ web thì khi tin tặc tấn công vào máy chủ phục vụ web có thể dẫn đến mã nguồn và cơ sở dữ liệu của ứng dụng đó bị xâm phạm. Do vậy, khi triển khai thực tiễn nên thiết kế tách biệt độc lập theo mô hình 3 lớp để tránh tình trạng một lớp bị tấn công và chiếm quyền kiểm soát dẫn đến các lớp khác bị ảnh hưởng. Việc phân loại độc lập 3 lớp như trên sẽ tạo điều kiện thuận lợi cho việc vận hành, bảo trì hệ thống cũng như dễ dàng áp dụng các biện pháp bảo vệ đối với mỗi lớp riêng biệt.

Trong trường hợp có khó khăn, hạn chế về nguồn lực xây dựng cổng/trang TTĐT thì vẫn nên áp dụng tối thiểu mô hình hai lớp với lớp cơ sở dữ liệu được tách biệt độc lập.

3.2. Triển khai hệ thống phòng thủ

3.2.1. Tổ chức mô hình mạng hợp lý

Việc tổ chức mô hình mạng hợp lý có ảnh hưởng lớn đến sự an toàn cho các cổng/trang TTĐT. Đây là cơ sở đầu tiên cho việc xây dựng các hệ thống phòng thủ và bảo vệ. Ngoài ra, việc tổ chức mô hình mạng hợp lý có thể hạn chế được các tấn công từ bên trong và bên ngoài một cách hiệu quả.



Hình 3. Mô hình mạng tổng quan

Trong một mô hình mạng hợp lý cần phải phân biệt rõ ràng giữa các vùng mạng theo chức năng và thiết lập các chính sách an toàn thông tin riêng cho từng vùng mạng theo yêu cầu thực tế:

- Vùng mạng Internet (hay Untrusted Network): còn gọi là mạng ngoài.
- Vùng mạng DMZ Network: Đặt các máy chủ cung cấp dịch vụ trực tiếp ra mạng Internet như web server, mail server, FTP Server, v.v...
- Vùng mạng Server Network (hay Server Farm): Đặt các máy chủ không trực tiếp cung cấp dịch vụ cho mạng Internet.
- Vùng mạng Private Network: Đặt các thiết bị mạng, máy trạm và máy chủ thuộc mạng nội bộ của đơn vị.

Một số khuyến cáo khi tổ chức mô hình mạng:

- Nên đặt các máy chủ web, máy chủ thư điện tử (mail server), v.v... cung cấp dịch vụ ra mạng Internet trong vùng mạng DMZ, nhằm tránh các tấn công mạng nội bộ hoặc gây ảnh hưởng tới an toàn mạng nội bộ nếu các máy chủ này bị cướp quyền điều khiển. Chú ý không đặt máy chủ web, mail server hoặc các máy chủ chỉ cung cấp dịch vụ cho nội bộ cơ quan trong vùng mạng này.
- Các máy chủ không trực tiếp cung cấp dịch vụ ra mạng ngoài như máy chủ ứng dụng, máy chủ cơ sở dữ liệu, máy chủ xác thực v.v... nên đặt trong vùng mạng server network để tránh các tấn công trực diện từ Internet và từ mạng nội bộ. Đối với các hệ thống thông tin yêu cầu có mức bảo mật cao, hoặc có nhiều cụm máy chủ khác nhau có thể chia vùng server network thành các vùng nhỏ hơn độc lập để nâng cao tính bảo mật.
- Nên thiết lập các hệ thống phòng thủ như tường lửa (firewall) và thiết bị phát hiện/phòng chống xâm nhập (IDS/IPS) để bảo vệ hệ thống, chống tấn công và xâm nhập trái phép. Khuyến cáo đặt firewall và IDS/IPS ở các vị trí như sau: đặt firewall giữa đường nối mạng Internet với các vùng mạng khác nhằm hạn chế các tấn công từ mạng từ bên ngoài vào; đặt firewall giữa các vùng mạng nội bộ và mạng DMZ nhằm hạn chế các tấn công giữa các vùng đó; đặt IDS/IPS tại vùng cần theo dõi và bảo vệ.
- Nên đặt một Router ngoài cùng (Router biên) trước khi kết nối đến nhà cung cấp dịch vụ internet (ISP) để lọc một số lưu lượng không mong muốn và chặn những gói tin đến từ những địa chỉ IP không hợp lệ.

3.2.2. Tổ chức các hệ thống phòng thủ

3.2.2.1. Firewall (Tường lửa)

Firewall là một thiết bị phần cứng hoặc một phần mềm hoạt động trong một môi trường máy tính nối mạng nhằm ngăn chặn những lưu lượng bị cấm bởi

chính sách an ninh của một cá nhân hay một tổ chức. Mục đích của việc sử dụng Firewall là:

- Bảo vệ hệ thống khi bị tấn công.
- Lọc các kết nối dựa trên chính sách truy cập nội dung.
- Áp đặt các chính sách truy cập đối với người dùng hoặc nhóm người dùng.
- Ghi lại nhật ký để hỗ trợ phát hiện xâm nhập và điều tra sự cố.

Cần thiết lập luật cho Firewall từ chối tất cả các kết nối từ bên trong Web Server ra ngoài Internet ngoại trừ các kết nối đã được thiết lập – tức là chỉ từ chối tất cả các gói tin TCP khi xuất hiện cờ SYN. Điều này sẽ ngăn chặn việc nếu như tin tặc có khả năng chạy các kịch bản mã độc trên Web Server thì cũng không thể cho các mã độc nối ngược từ Web Server trở về máy tính của tin tặc.

Tuy nhiên, hạn chế của Firewall là có thể làm chậm quá trình kết nối và trong một số trường hợp đối với một số người có hiểu biết thì có thể vượt qua được Firewall. Vì thế cần chú trọng đến việc bảo vệ hệ thống theo chiều sâu.

3.2.2.2. IDS/IPS (Thiết bị phát hiện/phòng, chống xâm nhập)

Các thiết bị IDS có tính năng phát hiện dấu hiệu các xâm nhập trái phép, còn các thiết bị IPS có tính năng phát hiện và ngăn chặn việc xâm nhập trái phép của tin tặc vào hệ thống. Như các thiết bị mạng, IDS/IPS cũng có thể bị tấn công và chiếm quyền kiểm soát và do đó bị vô hiệu hóa bởi tin tặc. Vì vậy cần thiết đảm bảo thực hiện một số tiêu chí khi triển khai và vận hành, gồm:

- Xác định công nghệ IDS/IPS đã, đang hoặc dự định triển khai.
- Xác định các thành phần của IDS/IPS.
- Thiết đặt và cấu hình an toàn cho IDS/IPS.
- Xác định vị trí hợp lý để đặt IDS/IPS.
- Có cơ chế xây dựng, tổ chức, quản lý hệ thống luật (rule).
- Hạn chế thấp nhất các tình huống cảnh báo nhầm (false positive) hoặc không cảnh báo khi có xâm nhập (false negative).

3.2.2.3. WAF (Tường lửa ứng dụng web)

Một WAF thường là một phần mềm, hay một thành phần nhúng được cài ngay trên máy chủ phục vụ web. Đôi khi WAF cũng được cung cấp như một thiết bị phần cứng có cài đặt sẵn phần mềm bên trong. WAF hoạt động bằng cách sử dụng một bộ lọc với các "luật" được định nghĩa trước hoặc do người dùng thêm vào để giám sát các dữ liệu trao đổi với ứng dụng web thông qua giao thức HTTP. Những quy tắc này có thể giúp phát hiện và chặn các truy vấn nhằm tấn công vào các lỗi phổ biến như Cross-site Scripting (XSS), SQL Injection, OS command Injection, Path Travesal,... cũng như một số lỗi khác

được nêu trong danh mục "OWASP Top 10" (http://en.wikipedia.org/wiki/Application_firewall)

Các dữ liệu đi vào hoặc đi ra khỏi ứng dụng web sẽ được WAF kiểm tra so sánh với các dấu hiệu được định nghĩa sẵn và quyết định cho phép dữ liệu đi qua hay chặn các dữ liệu đó lại. Đây là một quá trình lọc mà các thiết bị tường lửa lớp dưới không thực hiện được. Việc triển khai WAF sẽ phần nào hạn chế được các sai sót của người lập trình ứng dụng web. Các WAF nên được cài đặt giữa mỗi lớp trong kiến trúc web.

Xem thông tin tham khảo về các WAF tại Phụ lục II.

3.3. Thiết đặt và cấu hình hệ thống máy chủ an toàn

Để vận hành một máy chủ an toàn, việc cần lưu ý đầu tiên là luôn cập nhật phiên bản và bản vá mới nhất cho hệ thống. Ngoài ra, với mỗi loại máy chủ khác nhau sẽ có những biện pháp thiết đặt và cấu hình cụ thể để đảm bảo vận hành an toàn.

3.3.1. Hệ thống máy chủ Linux

- Đối với hệ thống cài đặt mới thì phải đảm bảo một số yêu cầu sau:
  + Khả năng hỗ trợ từ các bản phân phối (thông tin vá lỗi, thời gian cập nhật, nâng cấp, kênh thông tin hỗ trợ kỹ thuật).
  + Khả năng tương thích với các sản phẩm của bên thứ 3 (tương thích giữa nhân hệ điều hành với các ứng dụng, cho phép mở rộng module).
  + Khả năng vận hành và sử dụng hệ thống của người quản trị (thói quen, kỹ năng sử dụng, tính tiện dụng).
- Tối ưu hóa hệ điều hành về các mặt sau:
  + Chính sách mật khẩu: sử dụng cơ chế mật khẩu phức tạp (trên 7 ký tự và bao gồm: ký tự hoa, ký tự thường, ký tự đặc biệt và chữ số) nhằm chống lại các kiểu tấn công brute force.
  + Tinh chỉnh các thông số mạng: tối ưu hóa một số thông tin trong tập tin /etc/sysctl.conf.
  + Cho phép hoặc không cho phép các dịch vụ truy cập đến hệ thống thông qua hai tập tin /etc/hosts. allow và /etc/host.deny.
  + Gỡ bỏ các dịch vụ không cần thiết: việc gỡ bỏ các gói, dịch vụ không cần thiết sẽ hạn chế khả năng tiếp cận của kẻ tấn công và cải thiện hiệu năng của hệ thống.
  + Điều khiển truy cập: chỉ định các truy cập được phép đến hệ thống thông qua tập tin /etc/security/access.conf, /etc/security/time.conf,

/etc/security/limits.conf, giới hạn tài khoản được phép sử dụng quyền *sudo* thông qua tập tin /etc/pam.d/su.

+ Sử dụng kết nối SSH thay cho các kênh kết nối không an toàn như Telnet, FTP, v.v...
+ Quản lý hệ thống ghi nhật ký (log) một cách tập trung và nhất quán nhằm phục vụ cho mục đích điều tra khi có sự cố xảy ra.

3.3.2. Hệ thống máy chủ Windows

Máy chủ Windows được sử dụng khá phổ biến, việc bảo vệ cho máy chủ Windows là thực sự cần thiết. Để đảm bảo cho hệ thống cần thực hiện một số biện pháp sau:

- Đối với các dịch vụ và cổng:
  + Các dịch vụ đang chạy thiết lập với tài khoản có quyền tối thiểu.
  + Vô hiệu hóa các dịch vụ DHCP, DNS, FTP, WINS, SMTP, NNTP, Telnet và các dịch vụ không cần thiết khác nếu không có nhu cầu sử dụng.
  + Nếu là ứng dụng web thì chỉ mở cổng 80 (và cổng 443 nếu có SSL).
- Đối với các giao thức:
  + Vô hiệu hóa WebDAV nếu không sử dụng bởi ứng dụng nào hoặc nếu nó được yêu cầu thì nó phải được bảo mật.
  + Vô hiệu hóa NetBIOS và SMB (đóng các cổng 137, 138, 139, và 445).
- Tài khoản và nhóm người dùng:
  + Gỡ bỏ các tài khoản chưa sử dụng khỏi máy chủ.
  + Vô hiệu hóa tài khoản Windows Guest .
  + Đổi tên tài khoản Administrator và thiết lập một mật khẩu mạnh.
  + Vô hiệu hóa tài khoản IUSR_MACHINE nếu nó không được sử dụng bởi ứng dụng khác.
  + Nếu một ứng dụng khác yêu cầu truy cập anonymous, thì thiết lập tài khoản anonymous có quyền tối thiểu.
  + Chính sách về tài khoản và mật khẩu phải đảm bảo an toàn, sử dụng cơ chế mật khẩu phức tạp (trên 7 ký tự và bao gồm: ký tự hoa, ký tự thường, ký tự đặc biệt và chữ số).
  + Phải giới hạn Remote logons. (Chức năng này phải được gỡ bỏ khỏi nhóm Everyone).
  + Tắt chức năng Null sessions (anonymous logons).
- Tập tin và thư mục:

+ Tập tin và thư mục phải nằm trên phân vùng định dạng NTFS.
+ Tập tin nhật ký (log) không nằm trên phân vùng NTFS hệ thống.
+ Các nhóm Everyone bị giới hạn (không có quyền truy cập vào \Windows\system32).
+ Mọi tài khoản anonymous bị cấm quyền ghi (write) vào thư mục gốc.

- Tài nguyên chia sẻ:
  + Gỡ bỏ tất cả các chia sẻ không sử dụng (bao gồm cả chia sẻ mặc định).
  + Các chia sẻ khác (nếu có) cần được giới hạn (nhóm Everyone không được phép truy cập).
- Các phiên bản vá lỗi:
  + Cập nhật các phiên bản mới nhất.
  + Theo dõi thông tin cập nhật từ nhiều nguồn khác nhau.
  + Nên triển khai cập nhật trên hệ thống thử nghiệm trước khi cập nhật vào hệ thống thật.

3.3.3. Máy chủ web

3.3.3.1. Máy chủ IIS:

Máy chủ IIS được sử dụng khá phổ biến hiện nay trên các máy chủ Windows. Để bảo vệ cho máy chủ IIS cần thực hiện một số biện pháp sau:

- Nên sử dụng các giao thức mã hóa như SSL hoặc TLS nhằm mã hóa các kết nối an toàn.

- Cần thiết lập các thuộc tính trong Audit Policy trên máy chủ IIS trong môi trường làm việc đảm bảo toàn bộ thông tin của người dùng khi đăng nhập vào hệ thống sẽ đều được ghi lại. Tất cả những dữ liệu khi truy cập đều được ghi lại nhật ký.

- Cần thiết lập "*Deny access to this computer from the network*", với thiết lập này sẽ quyết định những tài khoản nào bị cấm truy cập tới máy chủ IIS từ mạng và các tài khoản người dùng sẽ bị hạn chế và đảm bảo tính bảo mật cao hơn. Sau đây là những tài khoản người dùng cần phải thiết lập chế độ cấm nêu trên: ANONYMOUS LOGON, Built-in Administrator và Guest.

- Nên tắt tất cả chi tiết thông báo lỗi mà có khả năng đưa ra quá nhiều thông tin. Việc đưa ra quá chi tiết các thông báo lỗi sẽ dẫn đến việc các tin tặc có thể lợi dụng để tìm hiểu thông tin về hệ thống.

- Nên cài đặt thư mục gốc của ứng dụng web trên phân vùng đĩa có định dạng NTFS, bởi vì khả năng kiểm soát quyền truy cập trên hệ thống tập tin với phân vùng định dạng NTFS mạnh hơn so với các định dạng FAT, FAT32. Khi

đã cài đặt thư mục gốc trên phân vùng NTFS thì cũng phải thiết lập quyền truy cập thấp nhất cho thư mục gốc này, tránh trường hợp thư mục gốc của ứng dụng web được mặc định là Everyone: Full Control.

- Trong IIS có rất nhiều thành phần (module) bổ trợ. Nên gỡ bỏ những thành phần không cần thiết ra khỏi IIS được cài đặt, vì những thành phần này khi bị lỗi có khả năng dẫn đến IIS bị tấn công và chiếm quyền kiểm soát một cách gián tiếp.

- Nên cài đặt URLScan để bổ sung thêm nhiều tính năng bảo mật cho IIS.

3.3.3.2. Apache HTTP:

Một số biện pháp cần thực hiện nhằm bảo vệ máy chủ Apache HTTP một cách an toàn:

- Tối ưu hóa việc sử dụng các thành phần (module) bằng việc gỡ bỏ những thành phần không cần thiết. Một số thành phần khuyến cáo nên gỡ bỏ ra khỏi Apache là: mod_userid, mod_info, mod_status, mod_include.

- Giới hạn các quyền truy cập: Tạo các tài khoản, nhóm người dùng riêng (khác root) để thực thi apache. Không cho phép sử dụng các tài khoản này để đăng nhập bằng cách chỉnh sửa nội dung trong tập tin passwd.

- Điều khiển truy cập: Sử dụng các chỉ mục (Directory) để điều khiển quá trình truy cập đến các thư mục hệ thống cần hạn chế quyền thâm nhập (ví dụ như các thư mục: root, admin, administrator). Không cho phép duyệt qua thư mục gốc (root). Cấu hình được thiết lập trong tập tin cấu hình httpd.conf:

```
<Directory/>
      order deny,allow
      deny from all
</Directory>
<Directory /www/htdocs>
      order allow,deny
      allow from all
</Directory>
```

- Hạn chế tối đa việc sử dụng các lựa chọn (option) sau: MultiViews, ExecCGI, FollowSymLinks, SymLinksIfOwnerMatch. Gỡ bỏ tất cả các trang html mặc định, hướng dẫn sử dụng, thông tin liên quan về web server, điều khiển Server Status, Server Information. Tắt chức năng HTTP TRACE. Bảo vệ các tập tin cấu hình .htaccess.

- Tổ chức quá trình ghi nhật ký: Cấu hình Error Log, Cấu hình Access Log theo một số gợi ý sau:

```
#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
```

```
#
LogLevel notice
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""_
combined
CustomLog log/access_log combined
```

- Đối với một số trang thông tin cần mã hóa truy cập có thể sử dụng qua SSL/TLS nhờ module mod_ssl.

- Hạn chế các thông tin về Web Server:

```
ServerTokens Prod
ServerSignature Off
```

- Điều chỉnh các thông số tối ưu: một số thiết lập tham khảo:

+ Thông số timeout:

```
Timeout 10
```

+ Thông số KeepAlive:

```
KeepAlive On
```

+ Thông số MaxKeepAliveRequests:

```
MaxKeepAliveRequests 100
```

+ Thông số KeepAliveTimeout:

```
KeepAliveTimeout 15
```

+ Thêm các thông số sau:

```
LimitRequestline 512
LimitRequestFields 100
LimitRequestFieldsize 1024
LimitRequestBody 102400
```

3.3.3.3. Apache Tomcat:

Một số biện pháp cần thực hiện nhằm bảo vệ máy chủ Apache Tomcat một cách an toàn:

- Gỡ bỏ các tài nguyên không liên quan: Trong quá trình cài đặt có thể xuất hiện các ứng dụng mẫu, tài liệu hướng dẫn và một số các thư mục không cần thiết khác. Vì vậy cần gỡ bỏ các tập tin, thư mục này nhằm hạn chế thấp nhất nguy cơ bị khai thác thông tin liên quan đến ứng dụng đang sử dụng:

```
$ rm -rf $CATALINA_HOME/webapps/js-examples \
$CATALINA_HOME/webapps/servlet-example \
$CATALINA_HOME/webapps/webdav \
$CATALINA_HOME/webapps/tomcat-docs \
$CATALINA_HOME/webapps/balancer \
$CATALINA_HOME/webapps/ROOT/admin \
$CATALINA_HOME/webapps/examples
```

- Giới hạn các thông tin về hệ thống:

+ Thay đổi thông tin server.info.

+ Tiến hành đóng gói lại tập tin CATALINA_HOME/server/lib/catalina.jar sau khi đã sửa đổi nội dung file ServerInfo.properties. Ví dụ:

```
cd CATALINA_HOME/server/lib
jar xf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

+ Trong tập tin ServerInfo.properties thay đổi giá trị server.info thành giá trị server.info=Apache Tomcat, sau đó đóng gói lại catalina.jar:

```
jar uf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

+ Thay đổi thông tin trong server.number. Thuộc tính thay đổi cũng tương tự như thông số server.info. Ví dụ:

```
cd CATALINA_HOME/server/lib
jar xf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

+ Trong tập tin ServerInfo.properties thêm thuộc tính server.number=<Version>, sau đó đóng gói lại catalina.jar:

```
jar uf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

+ Thay đổi thông tin trong server.built. Thuộc tính này cung cấp thông tin về thời gian mà Tomcat được biên dịch và đóng gói. Ví dụ:

```
cd CATALINA_HOME/server/lib
jar xf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

+ Trong tập tin ServerInfo.properties thêm thuộc tính server.built=< BuildDate>, sau đó đóng gói lại catalina.jar:

```
jar uf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

- Bảo vệ cổng shutdown:

+ Apache Tomcat sử dụng cổng 8005 để tiếp nhận các yêu cầu shutdown. Cập nhật thuộc tính shutdown trong tập tin server.xml ở $CATALINA_HOME/conf/server.xml:

```
<Server port="8005" shutdown="NOSHUTDOWN">
```

+ Hoặc bỏ chức năng shutdown trên cổng này:

```
<Server port="-1" shutdown="SHUTDOWN">
```

- Bảo vệ cấu hình Apache Tomcat:

+ Giới hạn truy cập đến $CATALINA_HOME: Gán quyền sở hữu cho tài khoản tomcat_admin:tomcat; gỡ bỏ các quyền đọc, ghi, thực thi; gỡ bỏ quyền ghi đối với nhóm:

```
chown tomcat_admin.tomcat $CATALINA_HOME
# chmod g-w,o-rwx $CATALINA_HOME
```

+ Giới hạn truy cập đến $CATALINA_BASE: Gán quyền sở hữu cho tài khoản tomcat_admin:tomcat; gỡ bỏ các quyền đọc, ghi, thực thi; gỡ bỏ quyền ghi đối với nhóm:

```
# chown tomcat_admin.tomcat $CATALINA_BASE
# chmod g-w,o-rwx $CATALINA_BASE
```

+ Giới hạn truy cập đến thư mục cấu hình Tomcat: Gán quyền sở hữu cho tài khoản tomcat_admin.tomcat; gỡ bỏ các quyền đọc, ghi, thực thi; gỡ bỏ quyền ghi đối với nhóm:

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf
# chmod g-w,o-rwx $CATALINA_HOME/conf
```

+ Giới hạn truy cập đến thư mục chứa các tập tin nhật ký (log): Gán quyền sở hữu cho tài khoản tomcat_admin:tomcat; gỡ bỏ các quyền đọc, ghi, thực thi:

```
# chown tomcat_admin:tomcat $CATALINA_HOME/logs
# chmod o-rwx $CATALINA_HOME/logs
```

+ Giới hạn truy cập đến thư mục chứa các tập tin thực thi: Gán quyền sở hữu cho tài khoản tomcat_admin:tomcat; gỡ bỏ các quyền đọc, ghi, thực thi:

```
# chown tomcat_admin:tomcat $CATALINA_HOME/bin
# chmod g-w,o-rwx $CATALINA_HOME/bin
```

+ Giới hạn truy cập đến thư mục chứa ứng dụng web: Gán quyền sở hữu cho tài khoản tomcat_admin:tomcat; gỡ bỏ các quyền đọc, ghi, thực thi:

```
# chown tomcat_admin:tomcat $CATALINA_HOME/webapps
# chmod g-w,o-rwx $CATALINA_HOME/webapps
```

+ Giới hạn truy cập đến tập tin context.xml: Gán quyền sở hữu cho tài khoản tomcat_admin:tomcat; gỡ bỏ các quyền đọc, ghi, thực thi; gỡ bỏ quyền ghi đối với nhóm:

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf/context.xml
# chmod g-w,o-rwx $CATALINA_HOME/conf/context.xml
```

+ Giới hạn truy cập đến tập tin logging.properties: Gán quyền sở hữu cho tài khoản tomcat_admin:tomcat; gỡ bỏ các quyền đọc, ghi, thực thi; gỡ bỏ quyền ghi đối với nhóm:

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf/logging.properties
# chmod g-w,o-rwx $CATALINA_HOME/conf/logging.properties
```

+ Giới hạn truy cập đến tập tin server.xml: Gán quyền sở hữu cho tài khoản tomcat_admin:tomcat; gỡ bỏ các quyền đọc, ghi, thực thi; gỡ bỏ quyền ghi đối với nhóm:

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf/server.xml
# chmod g-w,o-rwx $CATALINA_HOME/conf/server.xml
```

+ Giới hạn truy cập đến tập tin tomcat-users.xml: Gán quyền sở hữu cho tài khoản tomcat_admin:tomcat; gỡ bỏ các quyền đọc, ghi, thực thi; gỡ bỏ quyền ghi đối với nhóm:

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf/tomcat-users.xml
# chmod g-w,o-rwx $CATALINA_HOME/conf/tomcat-users.xml
```

+ Giới hạn truy cập đến tập tin web.xml: Gán quyền sở hữu cho tài khoản tomcat_admin:tomcat; gỡ bỏ các quyền đọc, ghi, thực thi; gỡ bỏ quyền ghi đối với nhóm:

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf/web.xml
# chmod g-w,o-rwx $CATALINA_HOME/conf/web.xml
```

3.4. Vận hành ứng dụng web an toàn

3.4.1. Kiểm tra hoạt động web an toàn

Để đảm bảo cho ứng dụng web vận hành an toàn, tránh được các nguy cơ tấn công từ bên ngoài hệ thống có thể tiến hành các bước cơ bản sau:

- Kiểm tra việc lộ thông tin nhạy cảm qua các công cụ tìm kiếm, bước này nhằm đảm bảo ứng dụng web sẽ không hiển thị các thông tin riêng như phiên bản, cấu trúc thư mục, v.v... lên kết quả của các công cụ tìm kiếm.

- Kiểm tra chức năng đăng xuất, đăng nhập có hoàn thành đúng nhiệm vụ hay không.

- Thiết đặt các quyền truy cập thích hợp vào các tập tin và thư mục nhạy cảm. Xóa các tập tin sao lưu dự phòng ra khỏi hệ thống.

- Sử dụng CAPTCHA và chế độ mật khẩu mạnh nhằm tránh trường hợp vượt qua CAPTCHA hay đoán được mật khẩu ngắn (không cho phép người dùng đặt mật khẩu yếu).

- Kiểm tra quá trình quản lý tài khoản và phiên của ứng dụng, việc truyền gửi những thông tin quan trọng như tên đăng nhập và mật khẩu cần được mã hóa nhằm tránh tình trạng nghe lén dữ liệu trên đường truyền. Bên cạnh đó việc cấp phát và mã hóa phiên đăng nhập cho người dùng cũng cần đảm bảo an toàn nhằm tránh tình trạng tin tặc đoán hay giả mạo phiên.

- Xác định loại mã nguồn hỗ trợ web (JSP, ASP, PHP,...) và kiểu framework phát triển web (mã nguồn mở, tự phát triển,...) để có biện pháp bảo vệ hợp lý cũng như cập nhật khắc phục các lỗ hổng được phát hiện.

- Xây dựng hoặc triển khai một hệ thống máy chủ Proxy dùng để chắc rằng các kết nối từ bên ngoài vào và từ bên trong ra sẽ được giám sát để tránh các mối đe dọa cũng như điều tra nguyên nhân khi hệ thống bị tấn công.

- Nếu có nhiều website được đặt chung trên máy chủ web, cần có biện pháp cách ly các website này ra, nhằm đảm bảo nếu có một website bị tấn công và chiếm quyền kiểm soát thì các website còn lại sẽ ít bị ảnh hưởng.

- Thiết kế trang báo lỗi chung để trả về cho tất cả các lỗi mà hệ thống có thể gặp phải. Biện pháp này nhằm giảm nguy cơ bị tấn công dựa theo thông báo lỗi của ứng dụng.

3.4.2. Khắc phục các lỗi phổ biến trên web

Trong trang web thường có các điểm cho người dùng nhập dữ liệu vào như mục "đăng nhập", mục "tìm kiếm", mục ID bài viết trên URL, v.v... Ngoài việc giúp cho người dùng dễ dàng tương tác với ứng dụng web, các mục này nếu không được quản lý chặt chẽ sẽ trở thành một nguy cơ lớn để thực hiện các cuộc tấn công vào ứng dụng web. Các dữ liệu bất hợp pháp nên được lọc trước để bỏ qua không đưa vào truy vấn trong cơ sở dữ liệu như các siêu ký tự, các biểu thức chính quy, các ký tự được mã hóa,... nhằm tránh cho ứng dụng trước những nguy cơ tấn công.

Có thể sử dụng biểu thức chính quy (áp dụng cho tất cả các ngôn ngữ lập trình) để thực hiện các công việc này. Ví dụ, sử dụng biểu thức chính quy để lọc các siêu ký tự:

```
w*((\|)|(\%7c)|(\<)|(\%3c)|(\%3e)|>|(`)|(\%60)|(&&)|(\%26\%26))
```

Hoặc để quy định giá trị mật khẩu nhập vào, ví dụ: cho phép mật khẩu từ 4 đến 8 ký tự gồm chữ thường và chữ hoa:

```
^(?=.*\d)(?=.*[a-z])(?=.*[A-Z]).{4,8}$
```

Cũng có thể sử dụng biểu thức chính quy để lọc tấn công Path Traversal:

```
\w*((\%5c)|(\/)|(\%2f)|(\\\))((\.\.)|(\%2e\%2e))
```

Hoặc lọc tấn công chia nhỏ hồi đáp HTTP (HTTP Response Splitting):

```
(((\%0d)+)((\%0a)+))+\w*(\:)
```

Trong số mười lỗi ATTT phổ biến trên cổng/trang TTĐT, mỗi lỗi sẽ có những biện pháp riêng để khắc phục như sau:

- *Tấn công Injection (bao gồm các kiểu tấn công như SQL* Injection, *OS Injection, LDAP Injection):*

  + Giới hạn quyền truy cập CSDL và phân quyền giữa các tài khoản người dùng, điều này giúp giảm khả năng khai thác CSDL của tin tặc ngay cả khi đã thực hiện thành công lệnh Injection.
  + Sử dụng thủ tục lưu trữ để đảm bảo các câu lệnh SQL từ ứng dụng được lưu trữ và triển khai ở máy chủ CSDL, điều này giúp cho dữ liệu do người dùng nhập vào không thể được tùy chỉnh dưới dạng một câu lệnh SQL. Để làm được điều này, ứng dụng phải được định dạng để sử dụng những thủ tục lưu trữ với giao diện an toàn như câu lệnh Callable của JDBC hay lệnh Object của ADO.
  + Sử dụng biểu thức chính quy để phát hiện tấn công SQL Injection:

Đối với các siêu ký tự:

```
(((\%3D)|(=))|((\%3C)|(\<))|((\%3D)|(\>)))[^\\n]*((\%27)|(\')|(\-\-)|(\%3B)|(;))
```

Với tấn công sử dụng từ khóa UNION:

```
((\%27)|(\'))(\W)*union
```

Với tấn công vào máy chủ MS SQL:

```
exec(\s|\+)+(s|x)p\w+
```

+ Sử dụng biểu thức chính quy để lọc tấn công LDAP Injection:

```
.(\)|\(|\||&)
```

- *Cross Site Scripting (XSS):*
  + Lọc tất cả các dữ liệu chưa tin tưởng một cách phù hợp dựa trên nội dung HTML.
  + Tạo một "danh sách trắng" để kiểm tra dữ liệu đầu vào một cách phù hợp.
  + Sử dụng biểu thức chính quy trong việc kiểm tra dữ liệu đầu vào để phát hiện tấn công XSS:

```
((\%3c)|<)[^\n]+((\%3e)|>)
```

- *Insecure Direct Object References (Tham chiếu trực tiếp đối tượng không an toàn):* Kiểm tra quá trình tham chiếu trực tiếp đến các tài nguyên hạn chế trên hệ thống để đảm bảo rằng người dùng bình thường không thể truy cập được các nguồn tài nguyên mà họ không có quyền truy cập. Nên sử dụng một cơ chế truy cập gián tiếp thay vì trực tiếp.

- *Cross Site Request Forgery (CSRF):* Việc ngăn chặn CSRF yêu cầu phải gộp những token không có khả năng đoán trước trong mỗi phiên giao dịch. Những token không những là duy nhất cho mỗi phiên người sử dụng mà còn duy nhất cho mỗi yêu cầu gửi đến ứng dụng.

- *Failure to Restrict URL Access (Thất bại trong việc hạn chế truy cập các URL quản trị):* Việc truy cập vào các URL có chức năng quản trị cần phải được kiểm tra thông qua quá trình xác thực và kiểm tra quyền của người dùng trước khi cho phép họ truy cập.

- *Bẻ gãy sự chứng thực và quản lý phiên:* Thiết đặt một phương pháp chứng thực và điều khiển phiên người sử dụng đủ mạnh để tránh khỏi bị những lỗi XSS mà có thể bị đánh cắp phiên sử dụng hoặc có thể giải mã phiên một cách dễ dàng.

- *Cấu hình bảo mật không an toàn:* Bảo mật một hệ thống nói chung phụ thuộc vào việc cấu hình bảo mật cho các thành phần riêng lẻ trong hệ thống như ứng dụng web, máy chủ web, hệ điều hành máy chủ, các thiết bị vật lý,... Tất cả các thiết đặt bảo mật này cần được xác định, thực hiện, bảo trì và tuyệt đối không nên sử dụng các cấu hình bảo mật mặc định có sẵn.

- *Chuyển hướng và chuyển tiếp không được kiểm tra:* Hạn chế sử dụng chuyển tiếp và chuyển hướng, nếu sử dụng thì phải có cơ chế chứng thực.

- *Lưu trữ mã hóa không an toàn:* Nhận biết nguy cơ và lên phương án bảo vệ đối với dữ liệu từ những tấn công bên trong hay bên ngoài, dữ liệu nhạy cảm phải luôn luôn mã hóa.

- *Thiếu sự bảo vệ lớp vận chuyển:* Cung cấp một cơ chế bảo vệ cho lớp vận chuyển bằng việc cấu hình SSL/TLS phù hợp.

3.5. Thiết đặt và cấu hình cơ sở dữ liệu an toàn

Việc thiết đặt và cấu hình cơ sở dự liệu an toàn là một quá trình phức tạp, đòi hỏi người quản trị phải hiểu rõ về cơ sở dữ liệu đang sử dụng. Để bảo vệ cho cơ sở dữ liệu an toàn cần thực hiện một số biện pháp sau:

- Luôn cập nhật phiên bản vá lỗi cho cơ sở dữ liệu mới nhất nhằm tránh các lỗi đã được công bố và khai thác.
- Gỡ bỏ các cơ sở dữ liệu không sử dụng.
- Gỡ bỏ hoặc vô hiệu hóa các thủ tục lưu trữ hoặc những hàm nhạy cảm có tương tác với hệ thống nhằm tránh việc tương tác đến hệ thống từ cơ sở dữ liệu.
- Tách biệt các cơ sở dữ liệu sử dụng cho mục các đích khác nhau.
- Khóa tất cả các kết nối từ hệ thống hoặc từ ứng dụng khác ngoài ứng dụng web và máy chủ web, không cho phép bất kỳ kết nối trực tiếp nào từ Internet đến database.
- Cấu hình ghi nhật ký và theo dõi nhật ký làm việc của cơ sở dữ liệu một cách hợp lý.
- Giới hạn truy cập đối với các tài khoản sử dụng (không có quyền xóa hoặc thay đổi cấu trúc cơ sở dữ liệu).
- Phân quyền cho các tài khoản và các tập tin hệ thống.
- Gỡ bỏ hoặc thay đổi các tài khoản mặc định và thiết lập mật khẩu mạnh cho các tài khoản đang sử dụng.
- Có cơ chế sao lưu dữ liệu và mã hóa các dữ liệu sao lưu.
- Sử dụng các công cụ để tìm kiếm lỗ hổng trên máy chủ SQL như MBSA (MS SQL).

3.6. Cài đặt các ứng dụng bảo vệ

3.6.1. Chống virus (Anti-Virus) và bảo vệ an toàn máy tính cá nhân

Việc cài đặt các ứng dụng bảo vệ như Anti-Virus có tác dụng rất lớn trong việc bảo vệ hệ thống. Chúng có thể hạn chế được việc bị cài thêm mã độc trong trường hợp kẻ tấn công đã xâm nhập được vào hệ thống, hoặc hạn chế việc

upload các mã độc khi ứng dụng web bị lỗi. Các chương trình Anti-Virus phải thỏa mãn yêu cầu sau:

- Luôn ở trạng thái đang hoạt động nhằm đảm bảo hệ thống luôn được bảo vệ.
- Đảm bảo tính toàn vẹn của tập tin và tài nguyên.
- Quét các mã độc đính kèm trong e-mail.
- Cập nhật dấu hiện nhận diện virus mới nhất.

Đối với máy tính cá nhân có thể xem xét cài đặt phần mềm bảo vệ an toàn máy tính tích hợp thường bao gồm cả chức năng chống virus, lọc tường lửa cá nhân. Xem Phụ lục 3 thông tin tham khảo về các phần mềm chống virus và bảo vệ an toàn máy tính cá nhân.

3.6.2. Hệ thống phát hiện xâm nhập máy tính (Host Based IDS)

Host Based IDS là hệ thống phát hiện xâm nhập máy tính (thường hay áp dụng đối với các máy chủ), đồng thời đưa ra cảnh báo về các hành động bất thường đối với tài nguyên trên hệ thống. Sử dụng Host Based IDS nhằm:

- Cảnh báo khi có sự thay đổi đối với mã nguồn ứng dụng.
- Cảnh báo khi có sự thay đổi đối với các tập tin hệ thống.
- Cảnh báo khi có sự thay đổi đối với các tập tin hệ thống.

3.7. Thiết lập cơ chế sao lưu và phục hồi

3.7.1. Cơ chế sao lưu

Sao lưu dữ liệu là điều kiện không thể thiếu khi triển khai các giải pháp kỹ thuật nhằm đảm bảo tính sẵn sàng của dữ liệu. Vì vậy khi thực hiện sao lưu cần xác định một số yêu cầu sau:

- *Phạm vi sao lưu:*

+ Sao lưu toàn bộ dữ liệu của hệ thống. Cơ chế này đảm bảo được tính toàn vẹn của dữ liệu và có thể phục hồi toàn bộ dữ liệu một cách nhanh chóng khi hệ thống bị sự cố. Tuy nhiên, đòi hỏi phải xây dựng một hệ thống sao lưu quy mô lớn.

+ Sao lưu từng phần riêng trong hệ thống. Cơ chế này nhằm phục hồi những phần gặp sự cố và không cần một hệ thống sao lưu quy mô lớn.

- *Thời gian sao lưu:*

Cần thiết lập một cơ chế sao lưu theo định kỳ (ngày, tuần, tháng,...) một cách tự động, nhằm đảm bảo việc sao lưu đầy đủ các dữ liệu theo yêu cầu.

- *Nội dung sao lưu:*

+ Sao lưu hệ điều hành máy chủ.

+ Sao lưu máy chủ web, Cơ sở dữ liệu, v.v...

+ Sao lưu thư mục và tập tin.

3.7.2. Cơ chế phục hồi

Tùy thuộc vào tình trạng hiện tại của hệ thống và cơ chế sao lưu đã được thiết lập mà lựa chọn cơ chế phục hồi dữ liệu cho hệ thống một cách thích hợp:

– Khôi phục nguyên trạng hệ thống.

– Khôi phục từng phần riêng biệt (hệ điều hành, cơ sở dữ liệu, các ứng dụng khác).

– Thường xuyên kiểm tra bản sao lưu để đảm bảo khả năng phục hồi thành công khi cần thiết.

4. ĐỐI PHÓ VỚI TẤN CÔNG TỪ CHỐI DỊCH VỤ

4.1 Tấn công từ chối dịch vụ:

- Tấn công từ chối dịch vụ (DoS) là kiểu tấn công vào hệ thống mạng bằng cách làm tăng đột biến lưu lượng băng thông, số lượng yêu cầu kết nối sử dụng dịch vụ vượt quá khả năng mà hệ thống có thể đáp ứng xử lý, dẫn đến dịch vụ của hệ thống hoạt động bị chậm, mất khả năng đáp ứng hoặc mất kiểm soát.

- Tấn công từ chối dịch vụ phân tán (DDoS) là dạng tấn công DoS nguy hiểm nhất khi nguồn tấn công nhiều và phân bố trên diện rộng trên mạng Internet toàn cầu, rất khó ngăn chặn triệt để. Thông thường các cuộc tấn công DDoS được gây ra bởi một số lượng khá lớn các máy tính trên mạng Internet bị điều khiển bởi tin tặc do nhiễm mã độc thường gọi là mạng botnet.

- Nguyên tắc chống tấn công DoS là cần phải lọc và gạt bỏ được các luồng tin tấn công, và tốt hơn nữa là ngăn chặn được các nguồn tấn công. Để chống DDoS phải vô hiệu hóa được hoạt động của các mạng botnet. Để làm được điều này một cách hiệu quả thường đòi hỏi các biện pháp điều phối ứng cứu sự cố ở quy mô quốc gia hay thậm chí phối hợp nhiều nước. Do đó khi phát hiện có các cuộc tấn công DoS hay DDoS, các đơn vị quản lý cổng/trang TTĐT cần báo cho Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) càng sớm càng tốt. Mặt khác, việc áp dụng các biện pháp và công cụ kỹ thuật tại chỗ để nâng cao năng lực bảo vệ các cổng/trang TTĐT cũng có hiệu quả rõ rệt.

4.2. Một số biện pháp kỹ thuật phòng chống tấn công từ chối dịch vụ:

- Tăng cường khả năng xử lý của hệ thống:
  + Tối ưu hóa các thuật toán xử lý, mã nguồn của máy chủ web,
  + Nâng cấp hệ thống máy chủ,

+ Nâng cấp đường truyền và các thiết bị liên quan,
+ Cài đặt đầy đủ các bản vá cho hệ điều hành và các phần mềm khác để phòng ngừa khả năng bị lỗi tràn bộ đệm, cướp quyền điều khiển, v.v...

- Hạn chế số lượng kết nối tại thiết bị tường lửa tới mức an toàn hệ thống cho phép.
- Sử dụng các tường lửa cho phép lọc nội dung thông tin (tầng ứng dụng) để ngăn chặn các kết nối nhằm tấn công hệ thống.
- Phân tích luồng tin (traffic) để phát hiện các dấu hiệu tấn công và cài đặt các tường lửa cho phép lọc nội dung thông tin (tầng ứng dụng) ngăn chặn theo các dấu hiệu đã phát hiện.

4.3. Một số công cụ kỹ thuật phòng chống tấn công từ chối dịch vụ:

Tùy khả năng đầu tư, các cổng/trang TTĐT có thể trang bị giải pháp hoặc sử dụng dịch vụ chống DoS/DDoS với các công cụ kỹ thuật sau:

- Sử dụng hệ thống thiết bị, phần mềm hoặc dịch vụ giám sát an toàn mạng (đặc biệt về lưu lượng) để phát hiện sớm các tấn công từ chối dịch vụ.
- Sử dụng thiết bị bảo vệ mạng có dịch vụ chống tấn công DDoS chuyên nghiệp kèm theo, ví dụ như: Arbor, Checkpoint, Imperva, Perimeter,...

PHỤ LỤC I. MƯỜI LỖI ATTT PHỔ BIẾN TRÊN CỔNG/TRANG TTĐT

1. ***Tấn công Injection***: bao gồm các lỗi cho phép thực hiện thành công các kiểu tấn công như SQL Injection, OS Injection, LDAP Injection. Kiểu tấn công này xảy ra khi người dùng gửi các dữ liệu không tin cậy đến ứng dụng web, những dữ liệu này có tác dụng như các câu lệnh với hệ điều hành hoặc các câu truy vấn với cơ sở dữ liệu nhằm phục vụ cho mục đích xấu.

2. ***Cross Site Scripting (XSS)***: Lỗi XSS xảy ra khi ứng dụng web nhận các dữ liệu độc hại và chuyển nó đến trình duyệt cho người dùng mà không xác nhận lại dữ liệu đó có hợp lệ hay không. Kiểu tấn công này cho phép kẻ tấn công thực thi các đoạn mã độc trong trình duyệt của nạn nhân và có thể cướp phiên người dùng hoặc chuyển hướng người dùng đến các trang độc hại khác.

3. ***Insecure Direct Object References (Tham chiếu trực tiếp đối tượng không an toàn)***: Việc tham chiếu xảy ra khi nhà phát triển ứng dụng web đưa ra tham chiếu đến một đối tượng bên trong ứng dụng như là một tập tin, một thư mục hay một khóa cơ sở dữ liệu. Nếu việc kiểm tra quá trình tham chiếu này không an toàn, kẻ tấn công có thể dựa theo để tham chiếu đến các dữ liệu mà họ không có quyền truy cập.

4. ***Cross Site Request Forgery (CSRF)***: là kiểu tấn công mà người dùng bị lợi dụng để thực thi những hành động không mong muốn ngay trên phiên đăng nhập của họ. Thông qua việc gửi người dùng một liên kết qua email hay chat, tin tặc có thể hướng người dùng thực thi một số hành động ngay trên trình duyệt của người dùng (như gửi bài viết, xóa bài viết, v.v...).

5. ***Failure to Restrict URL Access (Thất bại trong việc hạn chế truy cập các URL quản trị)***: Thông thường để vào được các đường dẫn quản trị thì ứng dụng phải kiểm tra người dùng có đủ quyền để truy cập vào đó hay không rồi mới hiển thị URL và các giao diện quản trị tương ứng khác. Để tránh tình trạng người dùng bình thường cũng truy cập vào các URL quản trị, mỗi lần truy cập vào các URL này cần được kiểm tra quyền kỹ càng, nếu không tin tặc có thể truy cập vào các URL này nhằm thực hiện các hành vi độc hại.

6. ***Bẻ gãy sự chứng thực và quản lý phiên***: Những chức năng của ứng dụng liên quan đến sự chứng thực và sự quản lý phiên làm việc thường không khởi tạo đúng, cho phép tin tặc tấn công mật khẩu, khóa và token của phiên làm việc hoặc khai thác lỗ hổng từ những sự khởi tạo này để gán định danh một người sử dụng khác.

7. ***Cấu hình bảo mật không an toàn***: là lỗi liên quan đến việc đặt cấu hình cho ứng dụng, framework, máy chủ web, ứng dụng máy chủ và platform sử dụng những giá trị thiết đặt mặc định hoặc khởi tạo và duy trì những giả trị không an toàn.

8. ***Chuyển hướng và chuyển tiếp không được kiểm tra***: Nhiều ứng dụng thường xuyên chuyển tiếp hoặc chuyển hướng người sử dụng đến những trang hoặc những website và sử dụng những dữ liệu chưa tin tưởng để xác định những trang đích. Không có sự kiểm tra phù hợp, tin tặc có thể chuyển hướng nạn nhân đến các trang giả mạo hoặc các trang có chứa mã độc, hoặc chuyển tiếp đến các trang web đòi làm thủ tục xác thực nhằm đánh cắp thông tin cá nhân.

9. ***Lưu trữ mã hóa không an toàn***: Ứng dụng web không có cơ chế bảo vệ hoặc tuy có cơ chế mã hóa và hashing (băm) dữ liệu để lưu trữ nhưng sử dụng không đúng cách đối với những dữ liệu quan trọng, như là thông tin thẻ tín dụng, thông tin cá nhân và những thông tin chứng thực. Do đó tin tặc có thể lợi dụng những kẽ hở này để đánh cắp những dữ liệu cần được bảo vệ.

10. ***Thiếu sự bảo vệ lớp vận chuyển***: Các ứng dụng không mã hóa dữ liệu khi truyền những thông tin quan trọng, hoặc nếu có mã hóa thì lại chỉ có thể sử dụng các chứng thực hết hạn hoặc không hợp lệ.

PHỤ LỤC 2. THÔNG TIN THAM KHẢO VỀ CÁC TƯỜNG LỬA

1. ***Firewall cứng***

+ Checkpoint (*http://www.checkpoint.com*)
+ Juniper (*http://www.juniper.net*)
+ Cisco (*http://www.cisco.com*)
+ Endian (*http://www.endian.com*)
+ Astaro (*http://www.astaro.com*)

2. ***Firewall mềm***

- Bản thương mại:
  + Microsoft Internet Security and Acceleration (ISA) Server (*http://www.microsoft.com*)
- Bản miễn phí (mã nguồn mở):
  + netfilter/iptables (*http://www.netfilter.org*)
  + pfSense (*http://www.pfsense.org*)
  + IPCop (*http://www.ipcop.org*)
  + Shorewall (*http://shorewall.net*)
  + SmoothWall (*http://www.smoothwall.org*)
  + Vyatta (*http://www.vyatta.org*)

3. ***Web Application Firewall (WAF)***

- Các phiên bản mã nguồn mở WAF phổ biến:
  + WebKnight (*http://www.aqtronix.com/?PageID=99*)
  + ModSecurity (*http://www.modsecurity.org*)
  + URLScan (*http://www.iis.net/download/urlscan*)
- Ngoài ra còn các bản WAF thương mại nổi tiếng sau:
  + Hyperguard (*http://www.artofdefence.com/en/products/hyperguard.html*)
  + WebDefend (*http://www.breach.com/products/webdefend.html*)
  + DotDefender (*http://www.applicure.com/*)
  + NetScaler application firewalls (*http://www.citrix.com*)
  + Eeye's SecureIIS (*http://www.eeye.com/Products/SecureIIS-Web-Server-Security.aspx*)
  + Appwall (*http://www.radware.com*)

ModSecurity: là phần mềm nguồn mở có thể hoạt động như một module trong máy chủ Apache hoặc là một thành phần độc lập. ModSecurity sử dụng biểu thức chính quy trong việc bảo vệ máy chủ web từ các cuộc tấn công được xác định trước dựa theo các dấu hiệu hoặc các cuộc tấn công bất thường khác. Bên cạnh đó, ModSecurity cũng có khả năng lọc các siêu ký tự do người dùng chèn vào ứng dụng web. Toàn bộ quá trình cài đặt và cấu hình có thể tham khảo thêm tại: *http://www.modsecurity.org/documentation*

URLScan: là một sản phẩm của Microsoft dành riêng cho các máy chủ web IIS. URL scan không chỉ bảo vệ máy chủ IIS 6 khỏi các điểm yếu từ các phiên bản cũ hơn mà còn cung cấp thêm các biện pháp bảo vệ khác như lọc dữ liệu mã hóa trên URL hoặc lọc các siêu ký tự do người dùng chèn vào để chống lại các loại tấn công như XSS, SQL Injection, v.v... Tham khảo cách cài đặt và sử dụng URLScan tại: *http://www.iis.net/download/urlscan*

PHỤ LỤC 3. THÔNG TIN THAM KHẢO VỀ CÁC PHẦN MỀM CHỐNG VIRUS VÀ BẢO VỆ AN TOÀN MÁY TÍNH CÁ NHÂN

1. ***Bản sản xuất trong nước:***

+ BKAV (*http://www.bkav.com.vn*)
+ CMC AntiVirus (*http://www3.cmcinfosec.com*)

2. ***Bản thương mại nước ngoài:***

+ AirScanner (*www.airscanner.com*)
+ BitDefender (*www.bitdefender.com*)
+ Computer Associates (*www.ca.com*)
+ F-Secure (*www.f-secure.com*)
+ Kaspersky (*www.kaspersky.com*)
+ McAfee (*www.mcafee.com*)
+ Symantec (*www.symantec.com*)
+ Trend Micro (*trendmicro.com*)
+ Avast (*www.avast.com*)
+ Avira (*www.avira.com*)

3. ***Bản miễn phí:***

+ Avast Free AntiVirus (*http://www.avast.com*)
+ Avira AntiVir Personal Free (*http://www.avira.com*)
+ Microsoft Security Essentials (*http://www.microsoft.com*)
+ Panda Cloud AntiVirus (*http://www.pandasecurity.com*)
+ Comodo Internet Security (*http://comodo.com*)
+ AVG AntiVirus (*http://www.free.avg.com*)