BỘ GIÁO DỤC VÀ ĐÀO TẠO
ĐẠI HỌC ĐÀ NẴNG

PHẠM THỊ HÀ PHƯƠNG

NGHIÊN CỨU XÂY DỰNG GIẢI PHÁP PHÒNG VỆ NGUY CƠ TRÊN ỨNG DỤNG WEB

Chuyên ngành: KHOA HỌC MÁY TÍNH
Mã số: 60.48.01

TÓM TẮT LUẬN VĂN THẠC SĨ KỸ THUẬT

Đà Nẵng - Năm 2011

Công trình được hoàn thành tại
ĐẠI HỌC ĐÀ NẴNG

Người hướng dẫn khoa học: **PGS. TS. Lê Văn Sơn**

Phản biện 1: **GS. TS. Nguyễn Thanh Thủy**

Phản biện 2: **TS. Huỳnh Hữu Hưng**

Luận văn được bảo vệ tại Hội đồng chấm Luận văn tốt nghiệp thạc sĩ kỹ thuật họp tại Đại học Đà Nẵng vào ngày 10 tháng 9 năm 2011.

** Có thể tìm hiểu luận văn tại:*

- Trung tâm Thông tin - Học liệu, Đại học Đà Nẵng
- Trung tâm Học liệu, Đại học Đà Nẵng

MỞ ĐẦU

1. Lý do chọn đề tài

Cùng với sự phát triển không ngừng của Internet, số lượng website và các dịch vụ đi kèm cũng tăng lên nhanh chóng. Khi khả năng quản lý và truy nhập thông tin của các website càng phát triển, thì càng có nguy cơ mất an toàn dữ liệu cho các website trong quá trình hoạt động. Phần lớn những nguy cơ này xuất phát từ các cuộc tấn công có mục đích để truy cập trái phép vào hệ thống nhằm khai thác hoặc thay đổi thông tin, phục vụ ý đồ của cá nhân hoặc tổ chức nhất định (gọi chung là tin tặc). Tuy nhiên, bên cạnh đó cũng còn có các nguy cơ khách quan khác như hệ thống gặp sự cố, người quản trị thiếu kiến thức về bảo mật,… Để đảm bảo cho sự vận hành của website cũng như bảo vệ những thông tin cá nhân của người dùng trang web, một vấn đề đặt ra là cần có giải pháp bảo vệ an toàn cho các website khỏi các nguy cơ nói trên.

Được sự đồng ý và hướng dẫn của PGS. TS. Lê Văn Sơn, tôi chọn thực hiện đề tài *"Nghiên cứu xây dựng giải pháp phòng vệ nguy cơ trên ứng dụng web"* với mong muốn đóng góp một giải pháp giúp bảo vệ toàn diện cho website khỏi các nguy cơ khách quan cũng như chủ quan trong quá trình vận hành ứng dụng web.

2. Mục đích nghiên cứu

Luận văn được thực hiện với mục đích nghiên cứu các nguy cơ khách quan cũng như chủ quan trên ứng dụng web. Qua đó xây dựng giải pháp phòng vệ nguy cơ, kiểm tra và khắc phục các nguy cơ.

3. Đối tượng và phạm vi nghiên cứu

Đối tượng nghiên cứu của đề tài là các nguy cơ phổ biến liên quan đến việc khai thác chức năng của ứng dụng web.

Phạm vi nghiên cứu của đề tài là xây dựng giải pháp phòng vệ nguy cơ trên ứng dụng web, bao gồm các giải pháp ở mức hệ thống và các giải pháp ở mức vận hành ứng dụng, tiếp đến là đề xuất giải pháp trong việc kết hợp sử dụng các công cụ kiểm tra lỗi bảo mật web.

4. Phương pháp nghiên cứu

Về lý thuyết, tìm hiểu ứng dụng web, sự vận hành của ứng dụng web và các nguy cơ liên quan đến ứng dụng web. Tiến hành phân loại nguy cơ, sau đó phân tích các nguy cơ phổ biến trên ứng dụng web gồm những lỗ hổng bảo mật nguy hại liên quan đến việc khai thác chức năng của ứng dụng. Qua đó đề xuất giải pháp kiểm tra và phòng tránh cho mỗi nguy cơ.

Về thực tiễn, nghiên cứu đề xuất giải pháp phòng vệ nguy cơ trên ứng dụng web, gồm các giải pháp ở mức hệ thống và các giải pháp ở mức vận hành ứng dụng. Tiếp đến là tìm hiểu các công cụ đã được phát triển để phục vụ cho việc đánh giá, kiểm tra các lỗi bảo mật web. Qua việc phân tích các ưu/khuyết điểm của mỗi công cụ, đề xuất một giải pháp tổng thể nhằm phát huy tối đa mọi ưu điểm của các công cụ, hạn chế thiếu sót trong kết quả đánh giá mà mỗi công cụ độc lập mang lại.

5. Ý nghĩa khoa học và thực tiễn của đề tài

Các kết quả nghiên cứu sẽ giúp người lập trình ứng dụng web và người vận hành trang web thông qua đó thực hiện quy trình phòng vệ nguy cơ cho ứng dụng web một cách tổng thể, bao gồm việc chủ động phòng tránh nguy cơ, kiểm tra sự xuất hiện của các nguy cơ và giải pháp khắc phục nếu đã gặp phải các nguy cơ đó.

6. Cấu trúc của luận văn

Bố cục của luận văn được tổ chức thành ba chương, có nội dung như sau:

Chương 1: Khái niệm về ứng dụng web và các nguy cơ trên ứng dụng web. Nghiên cứu kiến trúc cơ bản và hoạt động của một ứng dụng web, các vấn đề liên quan đến hoạt động của ứng dụng web. Tiếp đến, giới thiệu tổng quan về bảo mật web: số liệu thống kê về tình hình bảo mật, các nguy cơ ảnh hưởng đến bảo mật ứng dụng web và các phương pháp kiểm tra lỗi bảo mật web.

Chương 2: Phòng vệ nguy cơ trên ứng dụng web. Trình bày các nguy cơ phổ biến liên quan đến việc khai thác chức năng của ứng dụng web, đề xuất các giải pháp kiểm tra và phòng vệ cho từng nguy cơ. Bên cạnh đó giới thiệu giải pháp phòng vệ nguy cơ theo mô hình Defense-In-Depth, qua đó trình bày hướng tiếp cận và phát triển của đề tài trong việc xây dựng giải pháp phòng vệ nguy cơ trên ứng dụng web.

Chương 3: Triển khai giải pháp phòng vệ nguy cơ trên ứng dụng web. Nội dung chương này trình bày chi tiết việc triển khai xây dựng giải pháp phòng vệ nguy cơ cho ứng dụng web ở mức hệ thống và mức vận hành ứng dụng web. Ở mức hệ thống, triển khai xây dựng mô hình web an toàn. Ở mức vận hành ứng dụng, triển khai quy trình kiểm soát lỗi bảo mật ứng dụng web. Cuối cùng là minh họa việc áp dụng các giải pháp phòng vệ nguy cơ trên một trang web cụ thể qua việc kiểm tra mô hình web và các lỗi bảo mật trên trang web, sau đó đưa ra giải pháp phòng vệ nguy cơ cho trang web.

CHƯƠNG 1:
KHÁI NIỆM VỀ ỨNG DỤNG WEB VÀ CÁC NGUY CƠ TRÊN ỨNG DỤNG WEB

Nội dung chương này trình bày các khái niệm về ứng dụng web và các vấn đề liên quan đến bảo mật ứng dụng web. Nội dung khái niệm về ứng dụng web trình bày kiến trúc cơ bản của một ứng dụng web, các thành phần như lớp trình diễn, lớp ứng dụng, lớp cơ sở dữ liệu, và sự giao tiếp của các thành phần này trong hoạt động của ứng dụng web. Các vấn đề liên quan đến ứng dụng web trình bày các khái niệm liên quan đến sự vận hành của ứng dụng web như giao thức truyền dữ liệu HTTP/HTTPS, giao thức bảo mật SSL/TLS, các phương thức truyền dữ liệu GET/POST và sự quản lý phiên (session) trong quá trình giao tiếp giữa máy khách và máy chủ. Nội dung bảo mật ứng dụng web trình bày số liệu thống kê về tình hình bảo mật, các nguy cơ ảnh hưởng đến bảo mật ứng dụng web và các phương pháp được sử dụng để kiểm tra lỗi bảo mật web.

1.1 KHÁI NIỆM VỀ ỨNG DỤNG WEB

Một ứng dụng web thường bao gồm một tập hợp các kịch bản (script) cư trú ở máy chủ web (webserver) và tương tác với cơ sở dữ liệu (database) hay các nguồn nội dung động khác (dynamic content). Ứng dụng này nhanh chóng được sử dụng rộng rãi vì nó cho phép nhà cung cấp dịch vụ và khách hàng chia sẻ thông tin theo các nền độc lập thông qua cơ sở hạ tầng của Internet. Một vài ví dụ về ứng dụng web (web application) như: công cụ tìm kiếm, trang mua sắm và cổng thông tin điện tử hay máy chủ thư điện tử (webmail).

1.1.1 Kiến trúc cơ bản

Một ứng dụng web khi triển khai sẽ có ba lớp như sau: lớp trình diễn, lớp ứng dụng và lớp cơ sở dữ liệu. Trong đó:

- Lớp trình diễn tức là lớp nơi mà máy chủ được cài đặt có tác dụng phục vụ các yêu cầu về web, hay nói cách khác lớp trình diễn chính là máy chủ phục vụ web.
- Lớp ứng dụng là nơi các kịch bản hay mã nguồn (có thể là ASP.NET, PHP, JSP, Perl, Python, ...) phát triển ra ứng dụng web đó.
- Lớp cơ sở dữ liệu (có thể là MySQL, SQL Server, Oracle, …) là nơi mà ứng dụng lưu trữ và thao tác với dữ liệu của ứng dụng.

1.1.2 Hoạt động của một ứng dụng web

Đầu tiên trình khách (hay còn gọi là trình duyệt như Internet Explorer, Netscap Navigator,…) sẽ gửi một yêu cầu đến trình chủ web (Apache, Tomcat, IIS,…) thông qua các lệnh cơ bản GET, POST,… của giao thức HTTP/HTTPS. Trình chủ lúc này có thể cho thực thi một chương trình được xây dựng từ nhiều ngôn ngữ như Perl, C/C++,… hoặc trình chủ yêu cầu bộ diễn dịch thực thi các trang ASP, JSP,… theo yêu cầu của trình khách và thực hiện các yêu cầu như cập nhật, truy vấn thông tin trong cơ sở dữ liệu,… Sau đó ứng dụng web gửi thông tin lại cho người dùng qua trình duyệt.

1.2 CÁC VẤN ĐỀ LIÊN QUAN ĐẾN ỨNG DỤNG WEB

1.2.1 Nguồn gốc phát triển

1.2.2 Giao thức truyền dữ liệu (HTTP/HTTPS)

1.2.3 Giao thức bảo mật (SSL/TLS)

1.2.4 Phương thức truyền dữ liệu (GET/POST)

1.2.5 Sự quản lý phiên (session)

1.2.5.1 Session

1.2.5.2 Cookie

1.3 BẢO MẬT ỨNG DỤNG WEB

1.3.1 Tổng quan tình hình bảo mật ứng dụng web

1.3.1.1 Thông tin từ Zone-H.org

1.3.1.2 Thông tin từ sách trắng WHID (Web Hacking Incident Database - Cơ sở dữ liệu về sự cố tấn công web)

1.3.1.3 Thông tin từ VNCERT

1.3.2 Các nguy cơ trên ứng dụng web

1.3.2.1 Phân loại nguy cơ

Khi nghĩ đến phòng vệ nguy cơ cho ứng dụng web, người quản trị thường thực hiện các biện pháp chống lại sự tấn công của tin tặc. Tuy nhiên, những nguy cơ đe dọa đến an ninh của một ứng dụng web đến từ nhiều nguyên nhân khách quan, chủ quan khác nhau:

- Những thảm họa bất ngờ: bao gồm những tác động đến từ bên ngoài, ảnh hưởng đến bảo vệ ở mức vật lý của trang web như hỏa hoạn, bão lũ, động đất, khủng bố, tai nạn lao động,…
- Những sự cố máy tính: bao gồm những trục trặc vật lý ảnh hưởng đến hoạt động của trang web như sự cố nguồn điện, hỏng phần cứng, thiết bị nối mạng hỏng, môi trường vận hành thiết bị hỏng,…
- Những sự cố vô tình: bao gồm những ảnh hưởng đến hệ thống do yếu tố con người như nhân viên thiếu hiểu biết về bảo mật, nhân viên lơ đễnh cẩu thả khi quản lý hệ thống,…
- Những sự cố có chủ ý: bao gồm những hoạt động phá hoại, khai thác tấn công làm ảnh hưởng đến an ninh của trang web như tội phạm máy tính, tình báo công nghệ cao, khủng bố công nghệ cao, nhân viên bất mãn với tổ chức, nhân viên gián điệp bán thông tin để nhận hối lộ, nhân viên bị đánh lừa để lấy các tài khoản hệ thống (hay còn gọi là kỹ thuật xã hội – sociable engineer),…

Loại bỏ các mối đe dọa này đòi hỏi phải tốn nhiều thời gian và công sức. Vấn đề trước tiên là cần xây dựng ý thức rõ ràng và đầy đủ về những hiểm họa này, và sau đó lên kế hoạch thực hiện quản lý và phòng tránh rủi ro thích hợp trước mỗi loại nguy cơ.

1.3.2.2 Các nguy cơ phổ biến ảnh hưởng đến ứng dụng web

Như đã trình bày ở trên, các mối đe dọa ảnh hưởng đến an ninh của ứng dụng web đến từ nhiều nguyên nhân khác nhau. Mỗi nguy cơ cần có những biện pháp phòng tránh cụ thể. Trong khuôn khổ của luận văn này, tôi đi sâu tìm hiểu và đề xuất giải pháp phòng vệ cho các nguy cơ tấn công có chủ ý, hay nói cách khác chính là những nguy cơ tấn công từ phía tin tặc, tấn công nhắm mục tiêu dựa vào việc khai thác các điểm yếu trong sự vận hành của ứng dụng web. Các nguy cơ này được phân loại theo từng nhóm chức năng của ứng dụng web như sau:

- Lộ thông tin nhạy cảm.
- Quản lý xác thực không an toàn.
- Quản lý phiên không an toàn.
- Điều khiển truy cập không an toàn.
- Chèn dữ liệu không an toàn (dẫn đến lỗi XSS, SQLi,…).
- Tấn công từ chối dịch vụ (DOS).

Trên đây là các nguy cơ rất phổ biến và ảnh hưởng trực tiếp đến an toàn của ứng dụng, đòi hỏi phải có sự nghiên cứu, tìm ra giải pháp để kiểm tra và chủ động phòng vệ cho ứng dụng trước các nguy cơ.

1.3.3 Các phương pháp kiểm tra

Các phương pháp kiểm tra lỗi bảo mật trên ứng dụng web được dùng phổ biến là phương pháp kiểm tra hộp trắng và phương pháp kiểm tra hộp đen.

- Kiểm tra hộp trắng: là quá trình kiểm tra trực tiếp mã nguồn của ứng dụng web để tìm ra các lỗi bảo mật.
- Kiểm tra hộp đen: là phương pháp kiểm tra ứng dụng từ bên ngoài, tức là quan sát các dữ liệu được đệ trình đến ứng dụng và các dữ liệu từ ứng dụng xuất ra mà không cần hiểu đến hoạt động bên trong của ứng dụng.

Các phương pháp kiểm tra hộp trắng và hộp đen có thể được thực hiện một cách thủ công hoặc với sự hỗ trợ của các công cụ tự động. Phương pháp kiểm tra thủ công tuy đòi hỏi đầu tư nhiều thời gian và công sức nhưng giúp kiểm soát chặt chẽ mọi lỗi bảo mật khi vận hành ứng dụng. Để tăng cường hiệu suất của việc kiểm tra có thể sử dụng thêm các công cụ tự động. Tuy nhiên, cần kết hợp với sự hiểu biết của người kiểm tra trong quá trình sử dụng để giúp các công cụ tự động mang lại kết quả chính xác (đây là khái niệm liên quan đến kiểm tra hộp xám).

1.3.3.1 Kiểm tra thủ công

Kiểm tra thủ công là quá trình kiểm tra từng chức năng của ứng dụng, qua đó xác định được các điểm yếu bảo mật của ứng dụng để có giải pháp khắc phục phù hợp. Các công cụ hỗ trợ cho việc kiểm tra thủ công lỗi bảo mật: BURP, PAROS, WEBSCARAB,… Bằng việc sử dụng các công cụ này để quan sát hoạt động của ứng dụng trong việc thực hiện các request/response, người kiểm tra có thể phát hiện lỗi của ứng dụng để qua đó có biện pháp khắc phục lỗi cho ứng dụng.

1.3.3.2 Kiểm tra bằng công cụ tự động

Các công cụ tự động được phát triển để hỗ trợ cho việc kiểm tra thủ công các lỗi bảo mật trên ứng dụng web. Các công cụ này rất đa dạng, có thể là mã nguồn mở hoặc tính phí với các ưu/khuyết điểm

khác nhau. Những công cụ này sẽ tự động quét ứng dụng và phát hiện lỗi, sau đó trả về các báo cáo lỗi. Người kiểm tra lúc này cần phối hợp sử dụng nhiều công cụ để kiểm tra xác nhận lại những vị trí lỗi, tránh tình trạng công cụ cảnh báo lỗi sai hoặc thiếu. Các công cụ kiểm tra lỗi tiêu biểu như Acunetix, w3af,…

1.4 TỔNG KẾT CHƯƠNG 1

Trong toàn bộ chương 1, tôi đã giới thiệu tổng quan các vấn đề liên quan đến ứng dụng web và nguy cơ ảnh hưởng đến ứng dụng web.

Trình bày chi tiết về kiến trúc cơ bản của một ứng dụng web như lớp trình diễn, lớp ứng dụng, lớp cơ sở dữ liệu, và sự giao tiếp của các thành phần này trong hoạt động của ứng dụng web. Các khái niệm liên quan đến sự vận hành của ứng dụng web như giao thức truyền dữ liệu HTTP/HTTPS, giao thức bảo mật SSL/TLS, các phương thức truyền dữ liệu GET/POST và sự quản lý phiên (session) trong quá trình giao tiếp giữa máy khách và máy chủ.

Trình bày tổng quan về tình hình bảo mật web qua số liệu được tổng hợp từ nhiều nguồn thống kê uy tín như Zone-H hay sách trắng WHID (Web Hacking Incident Database) và số liệu về các cuộc tấn công vào các website ở địa phương, ở các cơ quan ban ngành tại Việt Nam do VNCERT cung cấp. Bên cạnh đó, trình bày các nguy cơ ảnh hưởng đến ứng dụng web và các phương pháp được sử dụng để kiểm tra lỗi bảo mật web.

Vấn đề đặt ra là các nguy cơ phổ biến trên ứng dụng web đến từ sự tấn công có chủ ý của tin tặc, tấn công nhắm mục tiêu dựa vào việc khai thác các điểm yếu trong vận hành của ứng dụng web, cần có sự nghiên cứu tìm ra giải pháp để kiểm tra và chủ động phòng vệ cho ứng dụng web trước các nguy cơ.

CHƯƠNG 2:
PHÒNG VỆ NGUY CƠ TRÊN ỨNG DỤNG WEB

Trong chương này, nghiên cứu việc phòng vệ các nguy cơ phổ biến trên ứng dụng web, việc phòng vệ toàn diện cho hệ thống, đồng thời giới thiệu hướng tiếp cận của luận văn trong việc xây dựng giải pháp phòng vệ nguy cơ trên ứng dụng web. Nội dung phòng vệ các nguy cơ phổ biến trình bày về các lỗ hổng bảo mật liên quan đến việc khai thác chức năng của ứng dụng web, như nguy cơ lộ thông tin nhạy cảm hay nguy cơ bị chèn các thông tin không đúng chuẩn để khai thác ứng dụng,… qua đó đề xuất các giải pháp kiểm tra và phòng vệ cho từng nguy cơ. Nội dung phòng vệ toàn diện cho hệ thống giới thiệu giải pháp phòng vệ nguy cơ theo mô hình Defense-In-Depth. Nội dung cuối của chương trình bày về việc xây dựng giải pháp phòng vệ nguy cơ trên ứng dụng web, các giải pháp này được phân tích từ các vấn đề liên quan đến mô hình ứng dụng web và các lỗi bảo mật trên ứng dụng web.

2.1 PHÒNG VỆ CÁC NGUY CƠ PHỔ BIẾN

2.1.1 Lộ thông tin nhạy cảm

2.1.1.1 Lộ mã nguồn

2.1.1.2 Lộ cấu trúc thư mục

2.1.1.3 Lộ tập tin cũ và tập tin sao lưu

❖ ***Biện pháp phòng tránh***

Kiểm tra sâu vào các tập tin nhạy cảm, sau đó có biện pháp bảo vệ cho các tập tin nhạy cảm này.

2.1.2 Vượt qua xác thực

Một vài trường hợp, chương trình xác thực có thể bị bỏ qua bằng cách gọi trực tiếp đến một trang nội bộ, tưởng rằng chỉ được truy cập sau khi đã xác thực thành công, hoặc giả mạo yêu cầu và

đánh lừa ứng dụng rằng xác thực đã thành công bằng cách sửa đổi các tham số URL cho trước.

❖ ***Biện pháp phòng tránh***

Có biện pháp xác thực phù hợp cho từng trang của ứng dụng.

2.1.3 Tấn công Brute Force

Các tài khoản người dùng khác nhau sẽ có những quyền truy cập vào hệ thống khác nhau. Tin tặc tìm cách liệt kê các User/Password hợp lệ và sau đó thực hiện tấn công Brute Force để tìm cặp User/Password hợp lệ.

❖ ***Biện pháp phòng tránh***

User/Password cần được đặt khó đoán và đảm bảo yêu cầu bảo mật như độ dài trên 7 ký tự, sử dụng các ký tự đặc biệt,…

2.1.4 Vượt qua xác quyền

Trang web có các phân quyền truy cập khác nhau cho các tài khoản người dùng khác nhau. Nếu một thành viên bên ngoài có thể đọc được những thông tin được bảo vệ không đúng quyền truy cập truy cập (vượt qua điều khiển truy cập) thì trang web đã không đảm bảo an ninh thông tin.

❖ ***Biện pháp phòng tránh***

Có biện pháp bảo vệ các đối tượng được truy cập bởi người dùng hoặc những tham chiếu đối tượng gián tiếp. Điều này ngăn chặn tin tặc trực tiếp truy cập những tài nguyên không được phép.

2.1.5 Leo thang đặc quyền

Leo thang đặc quyền xảy ra khi một người dùng được quyền truy cập vào một chức năng hoặc tài nguyên nhiều hơn mức được cho phép. Điều này thường gây ra bởi một lỗ hổng trong ứng dụng. Kết quả là ứng dụng cho phép các đặc quyền ngoài dự định của nhà phát triển hoặc quản trị viên hệ thống.

❖ ***Biện pháp phòng tránh***

Kiểm tra truy cập mỗi đối tượng sử dụng từ nguồn chưa tin tưởng phải có cơ chế kiểm tra điều khiển truy cập. Đảm bảo rằng người sử dụng đã chứng thực đối với những đối tượng được yêu cầu.

2.1.6 Lộ giá trị phiên

Các giá trị của một phiên làm việc gọi là các token gồm có cookie, định danh phiên (sessionID) và trường ẩn (hidden field). Nếu các giá trị của phiên bị lộ thì tin tặc có thể đóng giả là người dùng và truy cập được vào hệ thống với quyền của người sử dụng. Do vậy, cần phải luôn bảo mật các giá trị token này trong suốt quá trình liên lạc giữa người dùng và trình ứng dụng web.

❖ ***Biện pháp phòng tránh***

Có biện pháp bảo vệ các định danh phiên như sử dụng giao thức bảo mật SSL/TLS.

2.1.7 Chèn yêu cầu giả mạo (CSRF)

Tấn công CSRF (Cross Site Request Forgery – Chèn yêu cầu giả mạo) 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. Khi khai thác thành công lỗi CSRF, tin tặc có thể lấy được các thông tin về tài khoản người dùng, thực hiện các hành động làm nguy hại đến cơ sở dữ liệu trên trang web nếu người dùng đó là người quản trị trang web…

❖ ***Biện pháp phòng tránh***

Có thể gộp token duy nhất trong một trường ẩn. Nó sẽ được gửi thông qua phần thân của yêu cầu HTTP, tránh được việc gộp nó trong URL sẽ phơi bày cho tin tặc biết.

2.1.8 Chèn kịch bản thực thi (XSS)

Chèn kịch bản thực thi (Cross Site Scripting – XSS) là phương pháp thao tác với các thông số đầu vào để tìm ra lỗ hổng của ứng dụng. XSS cho phép tin tặc thực thi kịch bản trên trình duyệt của nạn nhân và có thể cướp đoạt phiên người sử dụng, thay đổi giao diện website hoặc chuyển hướng người sử dụng đến những trang độc hại.

❖ ***Biện pháp phòng tránh***

Có biện pháp lọc dữ liệu hợp lý để tránh tình trạng tin tặc chèn mã lệnh thực thi.

2.1.9 Chèn câu truy vấn SQL

Chèn câu truy vấn SQL (SQL Injection) là kiểu tấn công được thực hiện bằng cách chèn các câu truy vấn SQL vào dữ liệu tương tác giữa máy khách và trình ứng dụng. Quá trình khai thác lỗi SQL Injection thành công có thể giúp tin tặc lấy được các dữ liệu nhạy cảm trong cở sở dữ liệu, thực thi các hành động với quyền của người quản trị và cao hơn có thể điều khiển được hệ điều hành máy chủ.

❖ ***Biện pháp phòng tránh***

Kiểm tra dữ liệu đầu vào trước khi xử lý; Mã hóa dữ liệu trong cơ sở dữ liệu và không cho xuất trang báo lỗi nội dung cú pháp SQL để tin tặc không thể thu thập thông tin cơ sở dữ liệu; Giới hạn quyền truy cập cơ sở dữ liệu của người dùng và áp dụng các công nghệ phòng tránh lỗi SQL Injection,…

2.1.10 Tấn công từ chối dịch vụ

Tấn công từ chối dịch vụ là kiểu tấn công làm cho một trang web không thể được truy cập bởi người dùng bình thường. Tin tặc sử dụng một lượng lớn băng thông để làm lụt hệ thống máy chủ, làm cho máy chủ không đủ khả năng giải quyết tất cả các yêu cầu nhận được. Những kiểu tấn công này vượt xa tầm kiểm soát của các nhà

phát triển ứng dụng, và để giảm thiểu nguy cơ từ các cuộc tấn công này, chỉ có thể tăng cường kiến trúc mạng. Tuy nhiên, một vài lỗ hổng trong ứng dụng có thể bị lợi dụng để tấn công từ chối dịch vụ. Những vấn đề này thường nằm trong lỗi các trình ứng dụng và thường xuất phát từ điểm yếu trong việc kiểm tra các dữ liệu nhạy cảm do người dùng nhập vào.

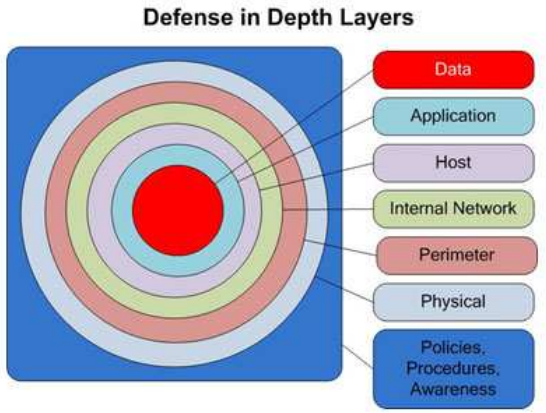
❖ ***Biện pháp phòng tránh***

Có biện pháp kiểm tra dữ liệu đầu vào trước khi xử lý.

2.2 PHÒNG VỆ TOÀN DIỆN HỆ THỐNG

Phòng vệ toàn diện hệ thống (Defense-In-Depth) là một chiến lược đảm bảo thông tin (IA – Information Assurance) trong đó các lớp được phòng vệ được đặt xuyên suốt trong hệ thống thông tin của một tổ chức. Mô hình này bao gồm việc phòng vệ nguy cơ cho hệ thống ở cả mức con người, công nghệ và vận hành. Đây là chiến lược được hình thành bởi Cơ quan An ninh quốc gia (Mỹ) – National Security Agency (NSA) để đảm bảo an ninh thông tin.

Mô hình Defense-In-Depth được trình bày như sau:



Hình 2.1. Các lớp trong mô hình Defense-In-Depth

Theo mô hình Defense-In-Depth, dữ liệu (Data) là thành phần quan trọng nhất trong một hệ thống web. Để bảo vệ lớp dữ liệu, các lớp bên ngoài được tổ chức như sau:

- Policies, Procedures, Awareness: bao gồm việc xây dựng các chính sách, thủ tục bảo mật, giáo dục ý thức về bảo mật.
- Physical: bảo vệ mức vật lý (ví dụ như sử dụng ổ khóa cửa).
- Perimeter: bảo vệ vành đai như tường lửa, cấu hình router, VPN,….
- Internal Network: bảo vệ mạng trong như các đoạn mạng, Network Based IDS,….
- Host: bảo vệ host như quản lý máy chủ, Host-Based Firewall, các phần mềm bảo vệ, hệ thống phòng thủ tấn công, quản lý việc cập nhật các lỗi bảo mật,….
- Application: bao gồm việc bảo vệ ở mức vận hành của ứng dụng như tạo mật khẩu mạnh, sử dụng các giao thức bảo mật như SSL/TLS, IPSec,…

2.3 ĐỀ XUẤT GIẢI PHÁP

2.3.1 Vấn đề về mô hình ứng dụng web

Một ứng dụng web khi được triển khai trên mạng Internet cần có sự tham gia của nhiều yếu tố. Để đảm bảo cho ứng dụng đó hoạt động an toàn thì các thành phần cấu thành như mã nguồn ứng dụng web phải được lập trình an toàn, các thành phần bổ trợ như máy chủ phục web và hệ quản trị cơ sở dữ liệu,… cũng cần được quản lý tốt. Tuy rằng không có một mô hình nào là tối ưu và đảm bảo an toàn tuyệt đối cho một ứng dụng web khỏi những nguy cơ, nhưng việc xây dựng một mô hình web hợp lý, cấu hình các thành phần trong mô hình web phù hợp với sự vận hành của ứng dụng là vấn đề trước tiên cần quan tâm để quản lý tốt hệ thống và giúp người quản trị chủ động

trong việc phòng chống cho ứng dụng trước các nguy cơ tấn công từ tin tặc.

2.3.2 Vấn đề về lỗi bảo mật trên ứng dụng web

Theo các kết quả thống kê đã được công bố, nghiên cứu tấn công và phòng thủ ứng dụng web là một lĩnh vực phát triển mạnh, trong đó các khái niệm mới và phương pháp tấn công mới được hình thành với tốc độ nhanh hơn so với các phương pháp cũ đã có. Mặt khác, việc phát triển không ngừng của công nghệ để áp dụng xây dựng các ứng dụng web đã được đẩy xa hơn nền tảng ban đầu rất nhiều. Chính điều này đã dẫn đến việc xuất hiện nhiều nguy cơ mới, kể cả những lỗ hổng bảo mật không lường trước được.

Tuy nhiên, các phương pháp tấn công hay nguy cơ mới xuất hiện xét cho cùng cũng xuất phát từ việc khai thác chức năng của hệ thống. Chính vì vậy để giải quyết vấn đề phòng vệ nguy cơ trên ứng dụng web, việc thường xuyên kiểm tra sự vận hành của ứng dụng, quá trình xử lý tốt thông tin vào/ra và quản lý thông tin trên hệ thống sẽ đáp ứng được yêu cầu đặt ra. Nói cách khác, việc xây dựng một quy trình kiểm soát chức năng của hệ thống cũng chính là để giải quyết vấn đề phòng vệ nguy cơ cho hệ thống.

2.3.3 Hướng tiếp cận và phát triển của đề tài

Như đã trình bày ở trên, để hạn chế các nguy cơ tấn công lên ứng dụng web, cần phải có một giải pháp tổng thể và được triển khai trên trên toàn bộ các lĩnh vực. Bắt đầu từ việc tuyên truyền ý thức, trách nhiệm về bảo mật; việc đào tạo đội ngũ quản trị, vận hành hệ thống đủ trình độ kỹ thuật; việc đầu tư hệ thống mạng, hệ thống phần cứng, phần mềm đảm bảo yêu cầu an ninh; việc xây dựng mô hình web hợp lý, đảm bảo yêu cầu an toàn cho hệ thống; đến việc kiểm soát tốt lỗi bảo mật trên ứng dụng web;…

Loại bỏ các yếu tố về tuyên truyền, đào tạo và đầu tư cho vấn đề bảo mật, trong khuôn khổ của luận văn, quan điểm "Xây dựng giải pháp phòng vệ nguy cơ trên ứng dụng web" được triển khai ở mức độ xây dựng mô hình ứng dụng web an toàn và kiểm soát tốt các lỗi bảo mật trên trang web.

- Vấn đề xây dựng mô hình ứng dụng web an toàn liên quan đến việc phòng vệ nguy cơ ở mức hệ thống của ứng dụng.
- Vấn đề kiểm soát các lỗi bảo mật trên ứng dụng web liên quan đến việc phòng vệ nguy cơ ở mức vận hành ứng dụng.

Các giải pháp phòng vệ nguy cơ này được xây dựng dưới góc nhìn của người lập trình ứng dụng web trong quá trình phát triển ứng dụng và người quản trị (admin) trang web trong quá trình vận hành ứng dụng.

2.4 TỔNG KẾT CHƯƠNG 2

Trong toàn bộ chương 2, tôi đã nghiên cứu việc phòng vệ các nguy cơ phổ biến trên ứng dụng web, phòng vệ toàn diện cho hệ thống, qua đó trình bày hướng tiếp cận của luận văn trong việc xây dựng giải pháp phòng vệ nguy cơ trên ứng dụng web.

Để phòng vệ các nguy cơ phổ biến trên ứng dụng web cần hiểu rõ về sự vận hành của ứng dụng web, qua đó tìm hiểu các lỗ hổng bảo mật liên quan đến việc khai thác chức năng của ứng dụng, sau đó là nghiên cứu về các giải pháp kiểm tra và phòng vệ cho từng nguy cơ.

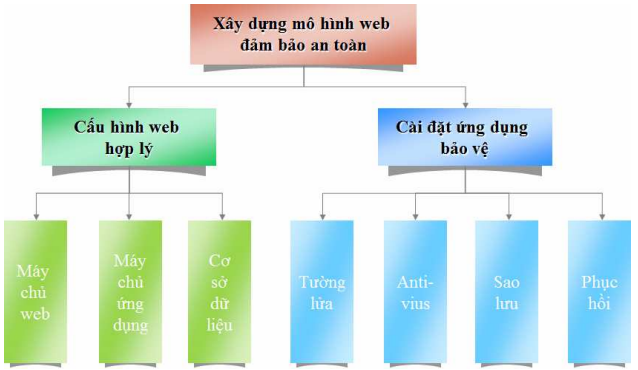
Bên cạnh đó để chủ động phòng tránh cho ứng dụng khỏi các nguy cơ cần có một giải pháp đảm bảo an toàn trên nhiều phương diện. Tôi đã giới thiệu mô hình Defense-In-Depth, qua đó đặt vấn đề về việc xây dựng giải pháp phòng vệ nguy cơ trên ứng dụng web ở mức hệ thống và mức vận hành ứng dụng web.

CHƯƠNG 3:
TRIỂN KHAI GIẢI PHÁP PHÒNG VỆ NGUY CƠ TRÊN ỨNG DỤNG WEB

Qua việc tìm hiểu các nguy cơ phổ biến liên quan đến việc khai thác chức năng của ứng dụng web, giải pháp phòng vệ nguy cơ cho ứng dụng web sẽ được triển khai xây dựng ở hai mức, mức hệ thống và mức vận hành ứng dụng web. Ở mức hệ thống, triển khai xây dựng mô hình web an toàn qua việc cấu hình các thành phần web hợp lý và việc cài đặt các ứng dụng bảo vệ cho trang web (như Firewall, Anti-vius,…). Ở mức vận hành ứng dụng web, triển khai quy trình kiểm soát lỗi bảo mật trên ứng dụng web. Cuối cùng là minh họa việc áp dụng các giải pháp phòng vệ nguy cơ trên website Bầu cử Quốc hội khóa 13 (baucukhoa13.quochoi.vn), cụ thể bằng việc kiểm tra mô hình web và các lỗi bảo mật trên trang web. Trên cơ sở đó, tôi báo cáo về các nguy cơ và giải pháp phòng vệ cho từng nguy cơ.

3.1 PHÒNG VỆ NGUY CƠ Ở MỨC HỆ THỐNG

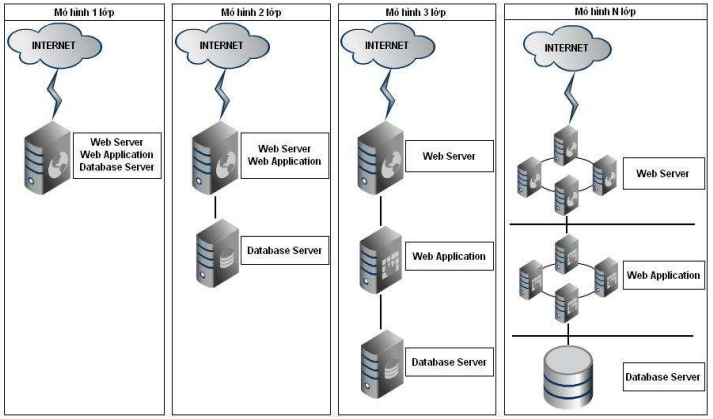
Để phòng vệ nguy cơ ở mức hệ thống, một mô hình web đảm bảo an toàn được đề xuất như sau:



Hình 3.1. Xây dựng mô hình web đảm bảo an toàn

3.1.1 Cấu hình web hợp lý

Một ứng dụng web khi triển khai sẽ có ba lớp: lớp trình diễn, lớp ứng dụng và lớp cơ sở dữ liệu. Việc hoạch định các lớp trong cấu trúc web tốt không những giúp cho người quản trị dễ dàng vận hành mà còn chủ động trong việc phòng chống các nguy cơ tấn công từ tin tặc. Một số cách bố trí lớp thường gặp trong thực tế như sau:



Hình 3.2. Các mô hình cấu trúc web

Qua các mô hình trên cho thấy nếu như triển khai giữa các lớp không có sự tách biệt rõ ràng thì một lớp bị tin tặc tấn công có thể dẫn đến các lớp khác cũng bị ảnh hưởng theo. Do vậy, các lớp khi triển khai nên tách biệt độc lập thành mô hình ba lớp, để tránh tình trạng một lớp bị tấn công dẫn đến các lớp khác bị ảnh hưởng. Ngoài ra, việc phân loại độc lập ba lớp 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 chuyên biệt.

3.1.2 Cài đặt ứng dụng bảo vệ

3.1.2.1 Firewall

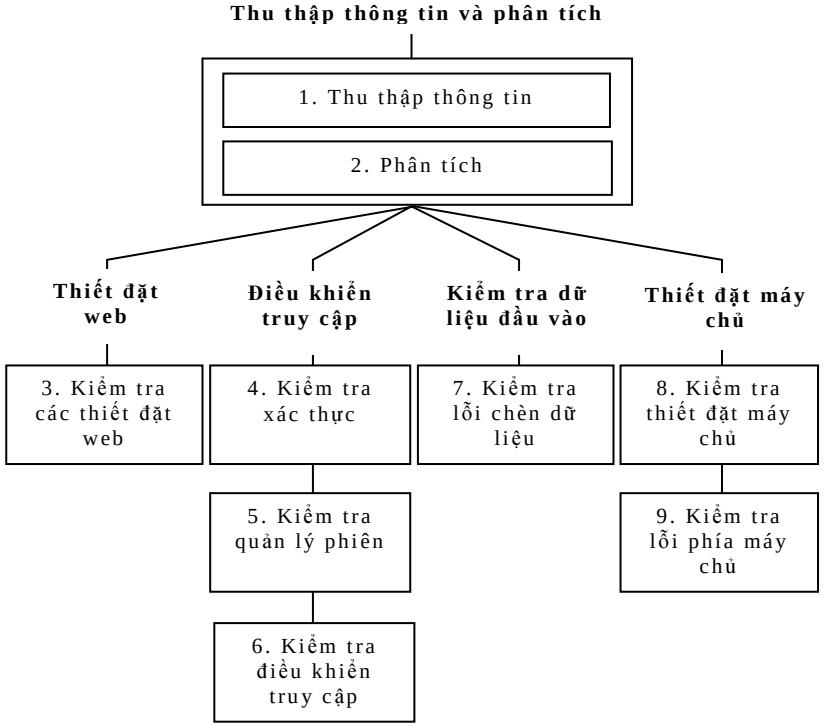
3.1.2.2 Anti-Virus

3.1.2.3 Cơ chế sao lưu

3.1.2.4 Cơ chế phục hồi

3.2 PHÒNG VỆ NGUY CƠ Ở MỨC VẬN HÀNH ỨNG DỤNG

Để phòng vệ nguy cơ ở mức vận hành ứng dụng, cần có một giải pháp kiểm tra mọi lỗi bảo mật liên quan đến hoạt động của ứng dụng web. Quy trình kiểm soát lỗi bảo mật trên ứng dụng web được tiến hành từ việc thu thập thông tin về ứng dụng web và tiến hành phân tích, đến việc kiểm tra các cấu hình và chức năng trên ứng dụng. Nội dung cụ thể như sau:



Hình 3.3. Quy trình kiểm soát lỗi bảo mật ứng dụng web

3.2.1 Thu thập thông tin

3.2.2 Phân tích điểm yếu ứng dụng

3.2.3 Kiểm tra thiết đặt web

3.2.4 Kiểm tra xác thực

3.2.5 Kiểm tra quản lý phiên

3.2.6 Kiểm tra điều khiển truy cập

3.2.7 Kiểm tra lỗi chèn dữ liệu

3.2.8 Kiểm tra thiết đặt máy chủ

3.2.9 Kiểm tra lỗi phía máy chủ

3.3 TRIỂN KHAI GIẢI PHÁP PHÒNG VỆ NGUY CƠ TRÊN WEBSITE BAUCUKHOA13.QUOCHOI.VN

3.3.1 Cài đặt công cụ

3.3.2 Báo cáo tổng quan

3.3.3 Báo cáo chi tiết lỗi

3.3.3.1 Lộ thông tin về hệ điều hành máy chủ và máy chủ web

3.3.3.2 Các giao thức được cho phép trên máy chủ

3.3.3.3 Tồn tại tập tin sao lưu trên website

3.3.3.4 Thư mục cơ sở dữ liệu tồn tại trên website

3.3.3.5 FTP hỗ trợ truy cập không mã hóa

3.3.3.6 Trang đăng nhập quyền quản trị không giới hạn số lần đăng nhập

3.3.3.7 Lỗi SQL Injection

3.3.3.8 Lỗi XPath Injection

3.3.3.9 Lỗi Cross Site Scripting (XSS)

3.3.4 Biện pháp phòng vệ nguy cơ

- Chỉ nên cho phép truy cập cổng 3389 từ mạng nội bộ hoặc đóng cổng này nếu không cần dùng để tránh các rủi ro lộ thông tin về máy chủ.

- Các tập tin sao lưu và tập tin cơ sở dữ liệu cần có biện pháp bảo vệ hợp lý, thiết lập các quyền truy cập với các tập tin này.
- Để đảm bảo an toàn trong quá trình truy cập FTP, nên sử dụng giao thức SFTP hoặc FTPS.
- Nên có chế độ khóa tài khoản hoặc địa chỉ IP nếu có số lần đăng nhập sai nhiều, hoặc sử dụng captcha tại nơi đăng nhập.
- Nên sử dụng một bộ lọc để kiểm tra tính hợp pháp của các siêu ký tự do người dùng nhập vào ứng dụng web để tránh các nguy cơ về lỗi chèn dữ liệu như SQL Injectiontion, XPath Injection hay Cross Site Scripting (XSS).

3.4 TỔNG KẾT CHƯƠNG 3

Trong toàn bộ chương 3, giải pháp phòng vệ nguy cơ cho ứng dụng web đã được triển khai xây dựng ở hai mức, mức hệ thống và mức vận hành ứng dụng web. Ở mức hệ thống, đã triển khai xây dựng mô hình web an toàn qua việc cấu hình các thành phần web hợp lý và việc cài đặt các ứng dụng bảo vệ cho trang web (như Firewall, Anti-vius,…). Ở mức vận hành ứng dụng web, đã triển khai quy trình kiểm soát lỗi bảo mật trên ứng dụng web. Quy trình này được xây dựng chi tiết từ mức thu thập thông tin, phân tích đến mức kiểm tra các hoạt động chức năng của ứng dụng web như kiểm tra các thiết đặt web, điều khiển truy cập, kiểm soát lỗi nhập liệu đầu vào và cuối cùng là kiểm tra các thiết đặt của máy chủ để đảm bảo an toàn cho hoạt động của ứng dụng web. Tôi cũng đã minh họa việc áp dụng các giải pháp phòng vệ nguy cơ trên vào việc kiểm tra website Bầu cử quốc hội khóa 13 với sự hỗ trợ của các công cụ được tập hợp trong BackTrack 5, qua đó đề xuất biện pháp phòng vệ nguy cơ cho trang web.

KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Từ kết quả nghiên cứu các tư liệu và thực nghiệm cho thấy các nguy cơ trên ứng dụng web được khai thác thành công dựa trên một nguyên tắc cơ bản là tin tặc cố gắng tìm kiếm các sai sót trong hoạt động của ứng dụng web và thông qua những sai sót này để tấn công ngược vào ứng dụng. Những sai sót (hay lỗ hổng bảo mật) này xuất hiện có thể có nhiều nguyên nhân: do bản thân ứng dụng trong quá trình phát triển đã để lại nhiều lỗ hổng nhưng chưa được kiểm tra kỹ lưỡng trước khi đưa vào vận hành, do ứng dụng chạy trên các nền tảng công nghệ chưa hoàn chỉnh được cung cấp bởi các nhà sản xuất và bị tin tặc thông qua đó khai thác để tấn công vào ứng dụng, do người quản trị hệ thống chưa hiểu rõ các nguyên tắc đảm bảo an toàn cho ứng dụng hoặc vô tình tạo ra các cơ chế quản lý lỏng lẻo, tạo điều kiện cho tin tặc tấn công,…

Kết quả thực hiện luận văn *"Nghiên cứu xây dựng giải pháp phòng vệ nguy cơ trên ứng dụng web"* tôi đã nghiên cứu về bảo mật ứng dụng web, các nguy cơ trên ứng dụng web và xây dựng hoàn thiện giải pháp phòng vệ nguy cơ trên ứng dụng web. Các nghiên cứu tổng quan về bảo mật ứng dụng web đã trình bày về hoạt động của ứng dụng web, các nguy cơ trên ứng dụng web cũng như các phương pháp thường được sử dụng để kiểm tra nguy cơ như kiểm tra thủ công hay kiểm tra bằng công cụ tự động. Nội dung phòng vệ nguy cơ trên ứng dụng web đã tập trung trình bày việc phòng vệ cho những nguy cơ phổ biến liên quan đến việc khai thác chức năng của ứng dụng web, mỗi nguy cơ đều trình bày từng giải pháp phòng vệ riêng và cuối cùng là trình bày về việc phòng vệ toàn diện cho hệ thống theo mô hình Defense-In-Depth. Từ việc nghiên cứu phòng tránh cho từng nguy cơ ảnh hưởng đến ứng dụng web, tôi đã đề xuất hướng

phát triển là cần phải có một giải pháp đảm bảo an toàn cho hoạt động của ứng dụng, qua đó sẽ tránh được các nguy cơ từ việc tin tặc khai thác những sai sót trong bản thân chức năng khi ứng dụng vận hành. Giải pháp phòng vệ nguy cơ trên ứng dụng web đã được triển khai xây dựng ở hai mức: mức hệ thống và mức vận hành ứng dụng. Ở mức hệ thống đã triển khai xây dựng mô hình web an toàn và ở mức vận hành ứng dụng đã triển khai quy trình kiểm soát lỗi bảo mật trên ứng dụng web.

Để đảm bảo an toàn cho ứng dụng web trước các hình thức tấn công ngày càng tăng cả về số lượng và chất lượng, không thể chỉ phụ thuộc vào một công nghệ hay một quy trình cụ thể vì công nghệ web đang phát triển nhanh chóng, kéo theo đó là nhiều khuyết điểm mới phát sinh. Sự tấn công không nằm trong khuôn khổ vài kỹ thuật đã phát hiện, mà linh động và tăng lên tùy vào những sai sót của nhà sản xuất, của người quản trị hệ thống cũng như của người lập trình ứng dụng web. Vấn đề thiết yếu cần quan tâm là bản thân người lập trình ứng dụng web hay người quản trị trang web cần có sự hiểu biết nền tảng về hoạt động của ứng dụng web, qua đó sẽ có những biện pháp thích hợp để cải tiến quy trình hay công nghệ kiểm soát lỗi bảo mật web một cách phù hợp. Các hướng phát triển nghiên cứu của luận văn như sau:

- Tiếp tục nghiên cứu những nguy cơ mới xuất hiện trên ứng dụng web và cách phòng vệ cho các nguy cơ trên nhằm nâng cao hiệu quả trong việc đảm bảo an toàn cho sự vận hành của ứng dụng web.
- Tìm hiểu thêm về các công cụ kiểm tra lỗi bảo mật mới được phát triển hoặc tự xây dựng một vài công cụ đặc thù hỗ trợ cho việc dò tìm lỗi bảo mật để phát huy tối đa hiệu quả của việc phòng vệ nguy cơ trên ứng dụng web.