BỘ GIÁO DỤC VÀ ĐÀO TẠO
ĐẠI HỌC ĐÀ NẴNG

ĐINH THỊ THIÊN ANH

NGHIÊN CỨU KIỂM THỬ BẢO MẬT WEBSITE`

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: TS Nguyễn Thanh Bình

Phản biện 1 : PGS.TS. Phan Huy Khánh

Phản biện 2 : PGS.TS. Lê Mạnh Thạnh

Luận văn đã được bảo vệ tại Hội đồng chấm Luận văn tốt nghiệp thạc sĩ kỹ thuật họp tại Đại học Đà Nẵng vào ngày 18 tháng 6 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

Với những nghiên cứu sinh theo đuổi quá trình học tập lên cao nữa, việc khởi đầu lựa chọn một đề tài thạc sỹ là rất quan trọng. Nó phải là đề tài mới, có hướng mở rộng chuyên sâu hay tiếp cận một vấn đề đã có theo một hướng khác tốt hơn cái đã có, đặc biệt là khả năng áp dụng thực tế và đem lại thiết thực trong cuộc sống.

Chính những lý do trên mà tôi mạnh dạn chọn đề tài: "Nghiên cứu kiểm thử bảo mật website".

2. MỤC TIÊU VÀ NHIỆM VỤ NGHIÊN CỨU

Nghiên cứu các vấn đề chung về các lỗi bảo mật, tiếp đến là các lỗi bảo mật liên quan đến các ứng dụng web. Trên cơ sở đó, xây dựng một quy trình kiểm thử bảo mật nhằm mục đích ứng dụng kiểm tra các lỗi bảo mật trên các ứng dụng web.

3. ĐỐI TƯỢNG VÀ PHẠM VI NGHIÊN CỨU

3.1. Đối tượng nghiên cứu

- Tìm hiểu chung về bảo mật, giới thiệu một số kiểu tấn công phổ biến hiện nay như DDos, SQLinjection, XSS.

- Giới thiệu một số công cụ hỗ trợ trong việc tìm ra các lỗi bảo mật như: Acunetix Web Vulnerability Scanner, Snort, NetCap, Power Injector 1.2.

- Tìm hiểu chung về các phương pháp kiểm thử bảo mật.

- Đề ra quy trình kiểm thử bảo mật nhằm ứng dụng vào các website.

- Các luận văn tốt nghiệp cao học.

3.2. Phạm vi nghiên cứu

Kiểm thử các lỗi bảo mật web, từ đó đề xuất xây dựng quy trình kiểm thử bảo mật nhằm ứng dụng kiểm thử các lỗi bảo mật web đối với các ứng dụng web đã hoàn thiện.

4. PHƯƠNG PHÁP NGHIÊN CỨU

- Nghiên cứu tổng quan về các lỗi bảo mật.
- Nghiên cứu những lỗi bảo mật ảnh hưởng đến ứng dụng web hiện nay.
- Nghiên cứu các quy trình, công cụ kiểm tra lỗi bảo mật web đã phát triển và đề xuất quy trình mới.

5. KẾT QUẢ DỰ KIẾN

- Tìm hiểu được một cách tổng quan về kiểm thử bảo mật.
- Đưa ra danh sách các phương pháp tấn công phổ biến hiện nay và các giải pháp nhằm hạn chế sự phá hoại của mỗi phương pháp tấn công.
- Xây dựng thành công quy trình kiểm thử bảo mật website ứng dụng vào website www.lat.com.vn.
- Là một tài liệu có chất lượng đóng góp vào quy trình đảm bảo chất lượng cho sản phẩm., giúp các nhà phát triển website hoàn thiện hơn sản phẩm của mình.

6. Ý NGHĨA KHOA HỌC VÀ Ý NGHĨA THỰC TIỄN CỦA LUẬN VĂN

6.1. Ý nghĩa khoa học

Luận văn không chỉ trình bày ngắn gọn nhưng đầy đủ các vấn đề chung về các lỗi bảo mật, mà còn đi sâu vào xây dựng quy trình kiểm thử bảo mật nhằm ứng dụng kiểm thử các lỗi bảo mật web đối với các ứng dụng web đã hoàn thiện.

6.2. Ý nghĩa thực tiễn

Sau khi thực hiện nghiên cứu kiểm thử các lỗi bảo mật trên ứng dụng web, sẽ góp phần giúp người phát triển ứng dụng web có thể kiểm tra ứng dụng của mình có bị mắc phải những lỗi bảo mật nào hay không. Từ đó, giúp người phát triển ứng dụng sẽ có những biện pháp cụ thể để giải quyết lỗi kịp thời.

7. BỐ CỤC CỦA LUẬN VĂN

Báo cáo luận văn được tổ chức thành 3 chương

CHƯƠNG 1 - TỔNG QUAN VỀ BẢO MẬT WEBSITE

1.1. TỔNG QUAN VỀ BẢO MẬT

Bảo mật là sự thỏa hiệp giữa bảo mật và chức năng / khả năng sử dụng. Nếu bảo mật của hệ thống quá chặt chẽ, nó sẽ trở nên rất khó sử dụng hoặc khó hoạt động một cách hiệu quả. Nếu bảo mật quá đơn giản, hệ thống dễ bị tấn công và xâm nhập.

Kiểm thử bảo mật Web, trong nghĩa truyền thống, là kiểm thử hiệu quả sự bảo vệ toàn bộ hệ thống Web. Nó yêu cầu kết hợp nhiều kiến thức về các công nghệ bảo mật, công nghệ mạng, lập trình, và kinh nghiệm thực tế về thâm nhập các hệ thống mạng. Hầu hết các kiểm thử viên phần mềm không có loại kiến thức này. Tuy nhiên, chúng ta nên hiểu các vấn đề về bảo mật sao cho chúng ta hiểu được các công việc chúng ta nên làm và các công việc nên được thực hiện bởi các chuyên gia khác.

1.2. MỤC ĐÍCH CỦA BẢO MẬT

Phụ thuộc vào các yêu cầu của mỗi hệ thống, mỗi hệ thống có những mục đích khác nhau, nhưng chúng đều có điểm chung là: Đảm bảo sự an toàn dữ liệu cho hệ thống và bảo vệ các tài nguyên

trên mạng trước sự tấn công nhằm phá vỡ hệ thống hoặc sử dụng trái phép các tài nguyên của một số người có chủ ý xấu.

1.3. THỐNG KÊ TÌNH TRẠNG BẢO MẬT HIỆN NAY

1.3.1. Tổng hợp thông tin từ các trang điện tử Việt Nam

1.3.2. Thông tin từ Zone-H.org

1.3.3. Thông tin từ WebAppSec.org

1.3.4. Thông tin từ Osvdb.org

1.4. MỘT SỐ PHƯƠNG PHÁP TẤN CÔNG PHỔ BIẾN HIỆN NAY

1.4.1. Tấn công SqlInjection

1.4.2. Tấn công Cross Site Scripting

1.4.3. Tấn công DOS

1.5. MỘT SỐ PHƯƠNG PHÁP TẤN CÔNG PHỔ BIẾN HIỆN NAY

1.5.1. Công cụ Acunetix Web Vulnerability Scanner

1.5.2. Công cụ Snort

1.5.3. Công cụ Netcat

***1.5.4.* Công cụ SQL Power Injection 1.2**

CHƯƠNG 2 – KIỂM THỬ BẢO MẬT

2.1. GIỚI THIỆU VỀ KIỂM THỬ PHẦN MỀM

Kiểm thử phần mềm được định nghĩa theo nhiều nguồn khác nhau, dưới đây một số định nghĩa phổ biến hiện nay

Kiểm thử phần mềm là quá trình khảo sát một hệ thống hay thành phần dưới những điều kiện xác định, quan sát và ghi lại các kết quả, và đánh giá một khía cạnh nào đó của hệ thống hay thành phần đó

Kiểm thử phần mềm là quá trình thực thi một chương trình với mục đích tìm lỗi.

Kiểm thử phần mềm là hoạt động khảo sát thực tiễn sản phẩm hay dịch vụ phần mềm trong đúng môi trường chúng dự định sẽ được triển khai nhằm cung cấp cho người có lợi ích liên quan những thông tin về chất lượng của sản phẩm hay dịch vụs phần mềm ấy. Mục đích của kiểm thử phần mềm là tìm ra các lỗi hay khiếm khuyết phần mềm nhằm đảm bảo hiệu quả hoạt động tối ưu của phần mềm trong nhiều ngành khác nhau.

2.2. KIỂM THỬ BẢO MẬT

2.2.1. Mục đích

Với tư cách là kiểm thử viên, là tập trung kiểm thử bảo mật của Website và ứng dụng Web ở mức ứng dụng. Điều đó có nghĩa là chúng ta tìm kiếm các lỗ hổng và rò rỉ thông tin gây nên chủ yếu do lập trình và do cấu hình sai các trình chủ Web và các trình chủ ứng dụng khác.

2.2.2. Trách nhiệm của kiểm thử bảo mật

Kiểm thử bảo mật liên quan đến trách nhiệm của nhiều nguồn khác nhau sau đây:

- Nhà định nghĩa chính sách (policymaker), định nghĩa các yêu cầu bảo mật nhằm tăng độ tin cậy của người sủ dụng và nhà sản xuất về bảo mật hệ thống.

- Người quản trị mạng, thiết kế và cài đặt các biện pháp bảo mật nhằm cung cấp bảo mật ở mức hoạt động.

- Lập trình viên phần mềm, chịu trách nhiệm kiểm thử hệ thống nhằm phát hiện các lỗi chức năng, tương tác cấu hình và khả năng tương thích khi họ liên quan đến cài đặt bảo mật (chủ yếu ở

mức ứng dụng và có thể ở mức hoạt động), phát hiện các vấn đề do lỗi thiết kế bảo mật.

- Các chuyên gia và nhà tư vấn bảo mật, giúp kiểm thử và duy trì các chương trình bảo mật cũng như xử lý các lỗ hỏng bảo mật. Thông thường, nhóm người này vốn trước đây là những kẻ tấn công. Những kẻ tấn công cũ, là những người có nhiều kinh nghiệm, chịu trách nhiệm điều khiển các kiểm thử xâm nhập trước khi triển khai một hệ thống. Trừ khi tổ chức của chúng tôi không có một chuyên gia để thực hiện kiểm thử xâm nhập, không nên để một kiểm thử viên và lập trình viên chịu trách nhiệm này.

2.2.3. Những ưu điểm trong kiểm thử bảo mật

- Kiểm thử bảo mật là kiểm thử chủ động, không bị động.

- Các lỗi không được xử lý là các kho báu để xác định các lỗ hỏng bảo mật.

- Các giao diện dữ liệu vào là các kho báu để chèn lỗi vào nhằm xác định các lỗi bảo mật.

+ Hãy xem xét mọi dữ liệu vào không hợp lệ có thể xảy ra phía trình khách.

+ Hãy xem xét mọi dữ liệu vào không hợp lệ có thể xảy ra phía trình chủ.

- Tập trung trên các điều kiện dữ liệu vào mà ở đó dữ liệu được chuyển từ miền không tin cậy vào miền tin cậy.

- Thiết kế các ca kiểm thử với sự nhấn mạnh trên các biên giữa các miền tin cậy và không tin cậy.

- Tìm kiếm các lỗi cho phép người sử dụng thực thi chương trình trên máy chủ.

- Tìm kiếm các lỗi cho phép người sử dụng tải chương trình trên máy chủ.

- Tìm kiếm các lỗi cho phép người sử dụng thay đổi nâng cao quyền truy cập.

- Luôn ý thức rằng ứng dụng thường xử lý sai một số dữ liệu xấu đến từ phía trình khách không tin cậy.

- Tìm kiếm dữ liệu vào mà có thể trở nên thực thi được (ví dụ: khi dữ liệu vào trở nên dữ liệu ra).

2.3. CÁC LOẠI KIỂM THỬ BẢO MẬT

2.3.1. Kiểm thử yêu cầu và thiết kế

Bất kỳ hệ thống nào cũng được xây dựng từ một tập hợp các yêu cầu. Đôi khi những yêu cầu này được viết một cách rõ ràng, nhưng thường chúng là những phát biểu mập mờ không được định nghĩa rõ ràng. Ví dụ, có thể có phát biểu "Ứng dụng phải an toàn". Nhưng "an toàn" nghĩa là gì và nên phải dành bao nhiêu công sức và thời gian để làm cho sản phẩm an toàn.

2.3.2. Kiểm thử mã nguồn

Phương pháp kiểm tra độ bảo mật của ứng dụng thông qua mã nguồn của ứng dụng. Phương pháp kiểm thử này chủ yếu dùng để xác định sự an toàn của thuật toán được dùng trong ứng dụng, xác độ nguy cơ rỏ rỉ thông tin, nguy cơ bị tấn công chiếm quyền kiểm soát thông qua mã nguồn. Phương pháp này thường ứng dụng kỹ thuật kiểm thử hộp trắng.

2.3.3. Kiểm thử các thiết lập của trình duyệt

Các thiết lập của trình duyệt có thể được cài đặt trong các trình duyệt như Mozilla FireFox và Microsoft Internet Explorer cho phép giới hạn truy cập đến các nội dung internet có thể gây hại. Người sử dụng sẽ thường có các chỉnh sửa các thiết lập này. Hơn nữa, có một sự thay đổi lớn phía người sử dụng về khả năng làm chủ các thiết lập này. Những người sử dụng Web ngày càng được đào tạo

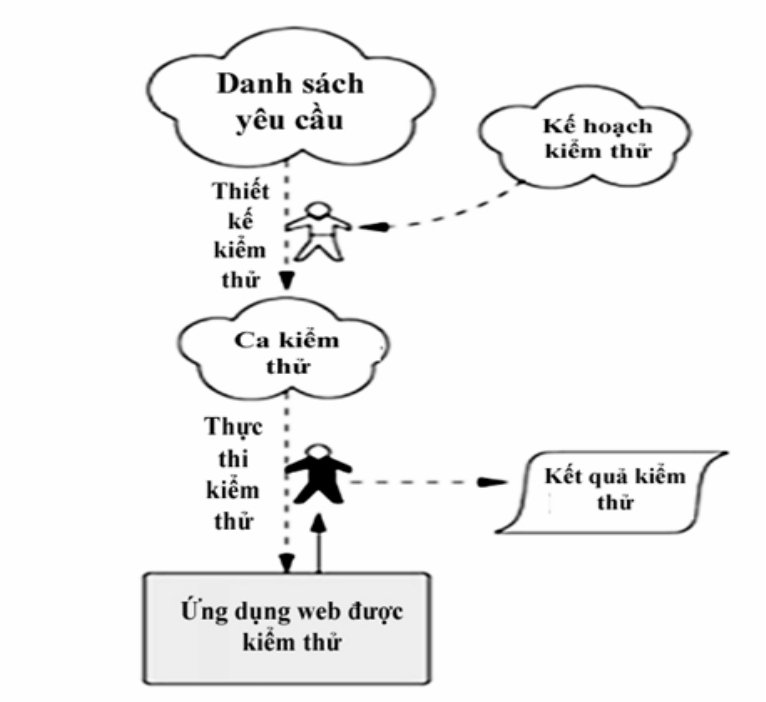
nhiều hơn cách sử dụng các thiết lập để bảo vệ chính họ. Với tư cách là một đội phát triển Website hay ứng dụng Web, chúng ta không thể bắt buộc người sử dụng chấp nhận các thiết lập mặc định. Vì vậy, chúng ta cần phải kiểm thử nhiều sự kết hợp của các thiết lập.

2.3.4. Kiểm thử bức tường lửa

Cần nhắc lại rằng nhóm kiểm thử phần mềm không chịu trách nhiệm kiểm thử sự hiệu quả của các tường lửa và sự cấu hình chúng. Kiểm thử tường lửa nhằm nhận biết các hiệu ứng về chức năng được tạo ra bởi sự chuyển dữ liệu qua các mạng khác nhau. Một số mạng riêng và một số khác công cộng.

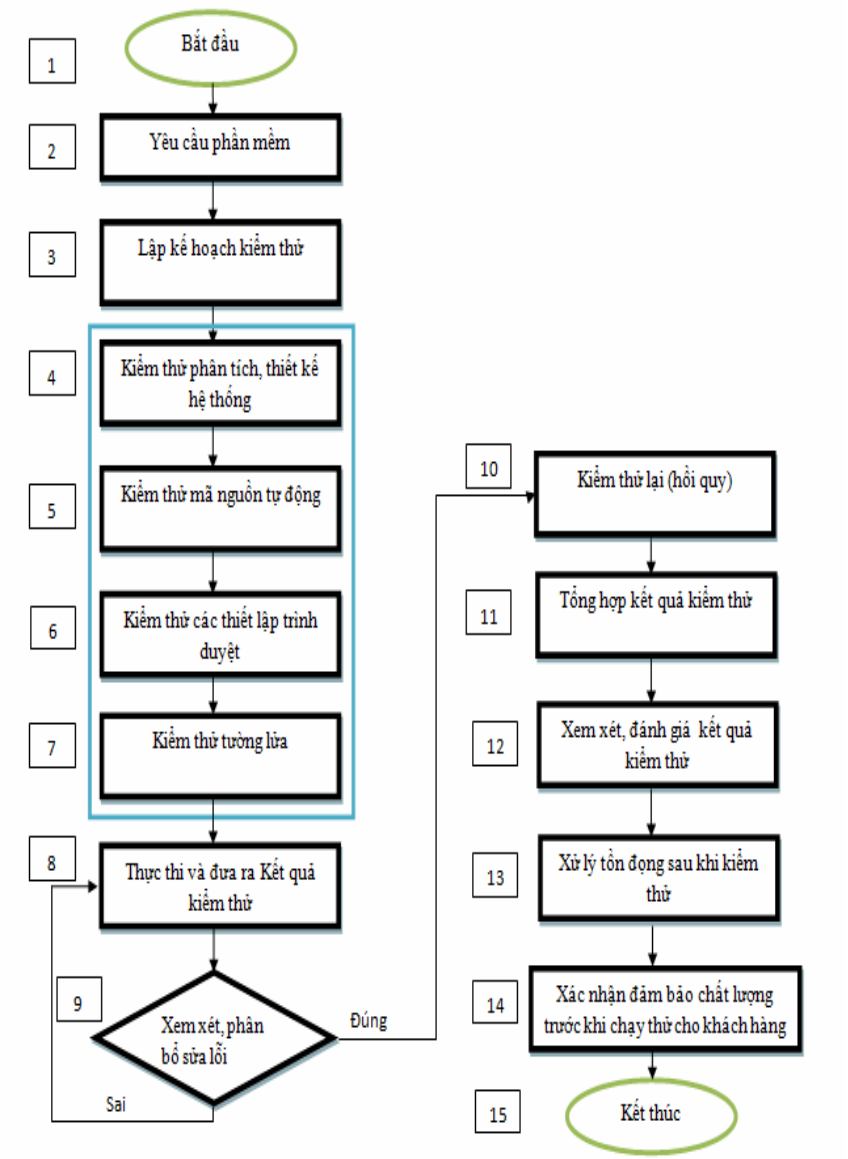
2.4. QUY TRÌNH KIỂM THỬ BẢO MẬT WEBSITE

2.4.1. Quy trình kiểm thử thủ công



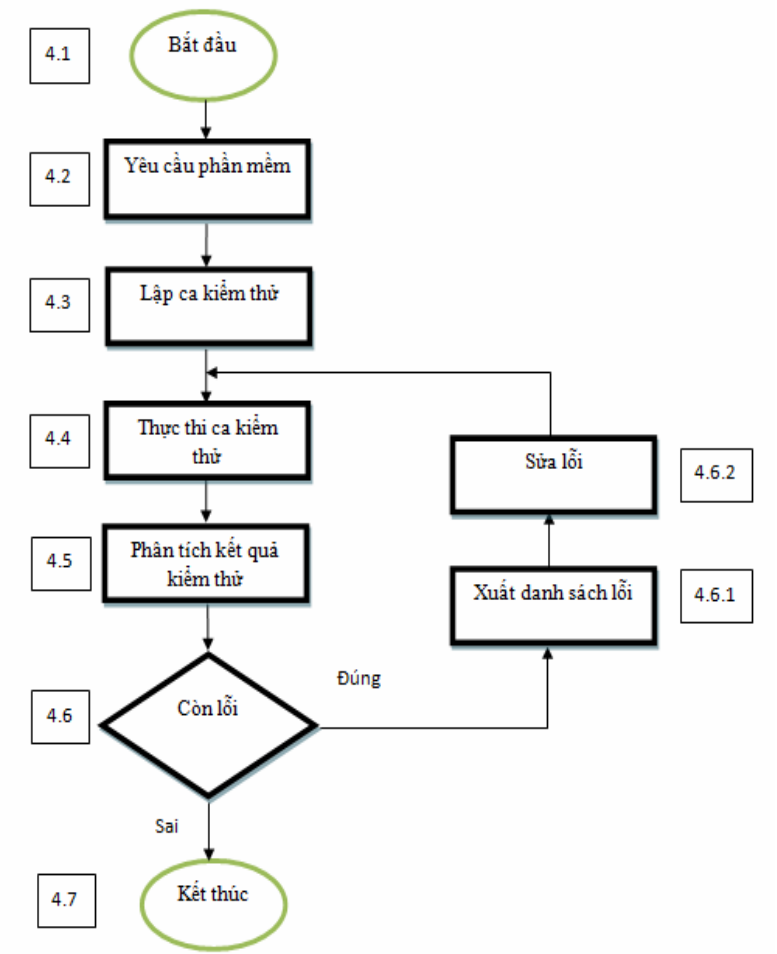
Hình 2.4: *Quy trình kiểm thử thủ công*

2.4.2. *Quy trình kiểm thử bảo mật đề xuất*



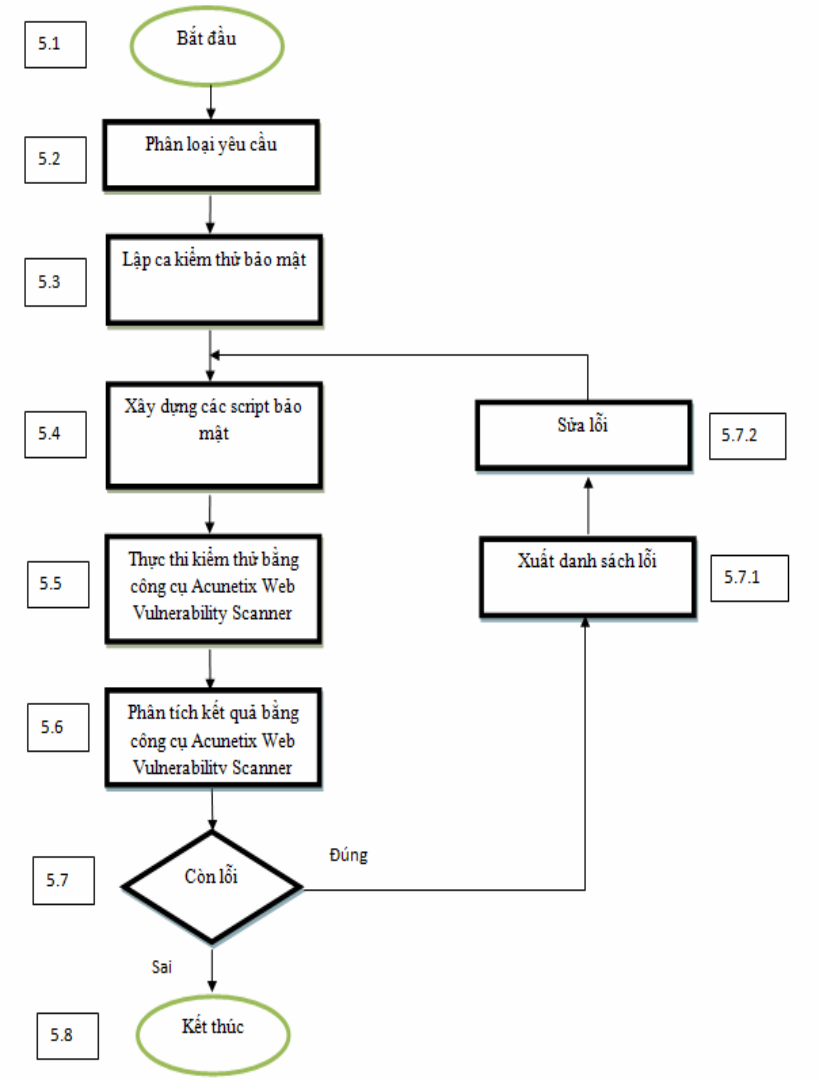
Hình 2.5: *Quy trình kiểm thử bảo mật đề xuất*

2.4.2.1. Mô hình kiểm thử bảo mật phân tích và thiết kế



Hình 2.6: *Mô hình kiểm thử bảo mật phân tích và thiết kế*

2.4.2.2. Mô hình kiểm thử mã nguồn tự động



Hình 2.7: *Mô hình kiểm thử bảo mật mã nguồn tự động*

CHƯƠNG 3 - ỨNG DỤNG KIỂM THỬ BẢO MẬT

3.1. GIỚI THIỆU WEBSITE WWW.LAT.COM.VN

Website LAT được thành lập năm 2009 với đội ngũ sáng tạo và năng động, website LAT ra đời mong muốn sẽ mang lại cho khách hàng những gì tốt đẹp nhất, những dịch vụ hoàn hảo nhất. LAT gồm có những dịch vụ cơ bản sau:

1. Thiết kế và xây dựng website cho doanh nghiệp.

2. Tư vấn xây dựng hệ thống thông tin, tin học hóa cho doanh nghiệp.

3. Tư vấn xây dựng và thiết kế hệ thống.

4. Xây dựng các sản phẩm phần mềm như: Hệ thống quản lý nhân sự, chấm công, tiền lương, giải pháp quản lý bán hàng, giải pháp quản lý khách sạn, nhà hàng,..

5. Đào tạo nguồn nhân lực công nghệ thông tin, chủ yếu là phát triển phần mềm.

6. Đào tạo chuyên viên công nghệ thông tin, soạn giáo trình điện tử... cho các trường đại học và cao đẳng.

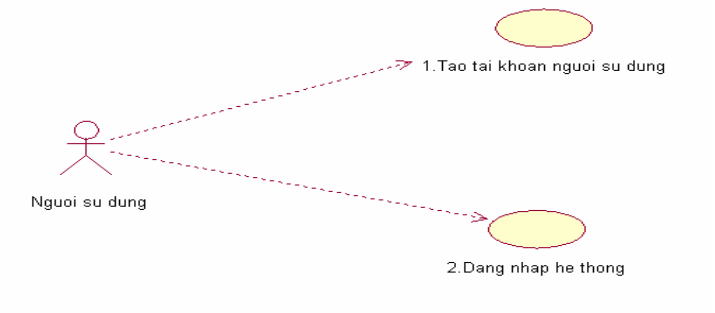
3.2. YÊU CẦU CHỨC NĂNG CỦA WEBSITE WWW.LAT.COM.VN

Bảng 3.1: *Bảng nội dung yêu cầu chức năng website www.lat.com.vn*

STT	Tên chức năng	Mô tả chức năng
1	Trang chủ	Được thiết kế ấn tượng, hiện đại, các chức năng nổi bật được hiển thị ngay tại trang chủ như: giới thiệu sơ lượt về LAT, các dịch vụ thiết kế website, phần mềm,…
2	Giới thiệu	Giới thiệu thông tin tổng quan về LAT, lịch sử hình thành.
3	Đào tạo	Chức năng này cung cấp cho người quản trị một trình soạn thảo để người quản trị có thể cập nhật các chương trình đào tạo của nhóm.
4	Tư vấn web và ứng dụng	Chức năng cho phép người quản trị viết các bài viết tư vấn về công nghệ thông tin hoặc là bài sưu tầm chuyên về web hoặc ứng dụng.
5	Dự án đã làm	Giới thiệu các dự án đã làm đến khách hàng của LAT.
6	Tài liệu	Cung cấp những thư viện tài liệu liên quan đến lập trình hỗ trợ người dùng.
7	Thông tin liên hệ	Thông tin liên lạc của LAT.
8	Hỗ trợ trực tuyến	Hỗ trợ khách truy cập thông qua các phần mềm chat thông dụng trên internet như YM, Skype…
9	Thống kê lượt truy cập	Thông tin về số lượt truy cập website.
10	Quản trị hệ thống	Quản trị Tài khoản/Phân quyền. Công cụ quản trị toàn bộ thông tin và sản phẩm của các chức năng.

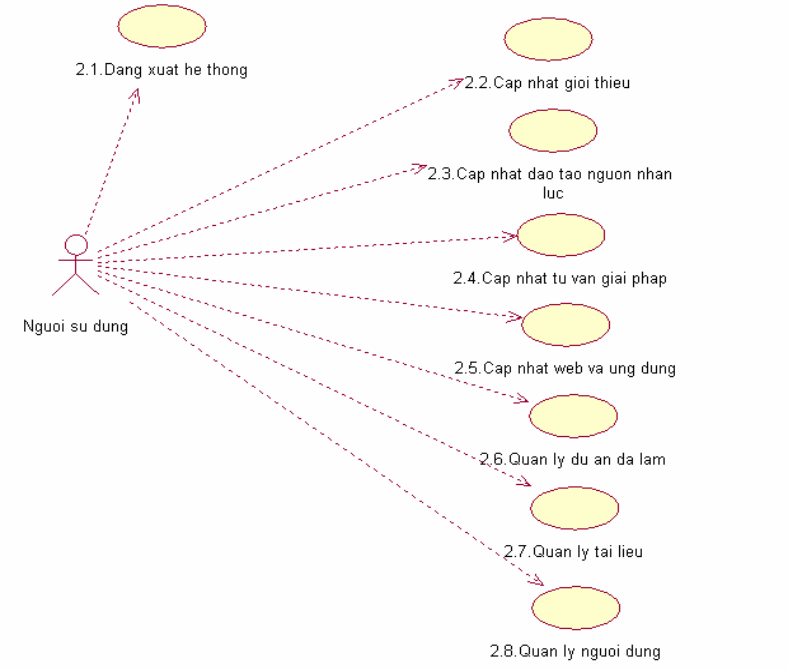
3.3. BIỂU ĐỒ CA SỬ DỤNG

3.3.1. Biểu đồ ca sử dụng trước khi đăng nhập vào hệ thống



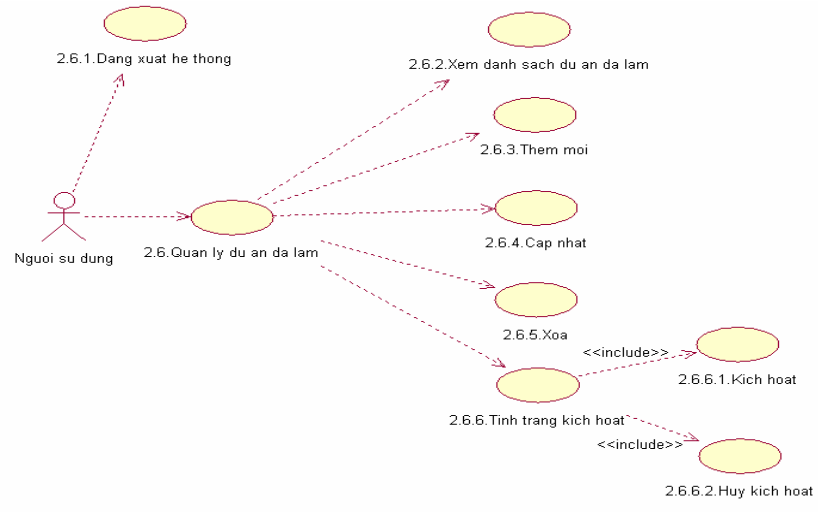
Hình 3.1: *Biểu đồ ca sử dụng trước khi đăng nhập vào hệ thống*

3.3.2. Biểu đồ ca sử dụng sau khi đăng nhập vào hệ thống



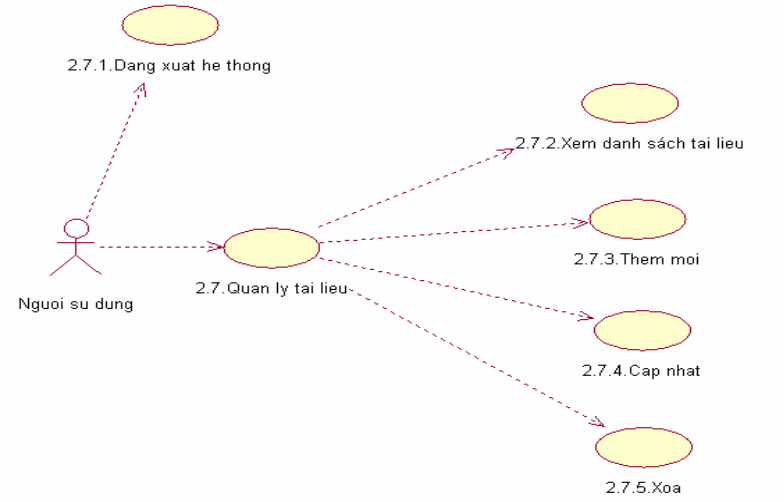
Hình 3.2: *Biểu đồ ca sử dụng sau khi đăng nhập vào hệ thống*

- Biểu đồ ca sử dụng 2.6. Quản lý dự án đã làm



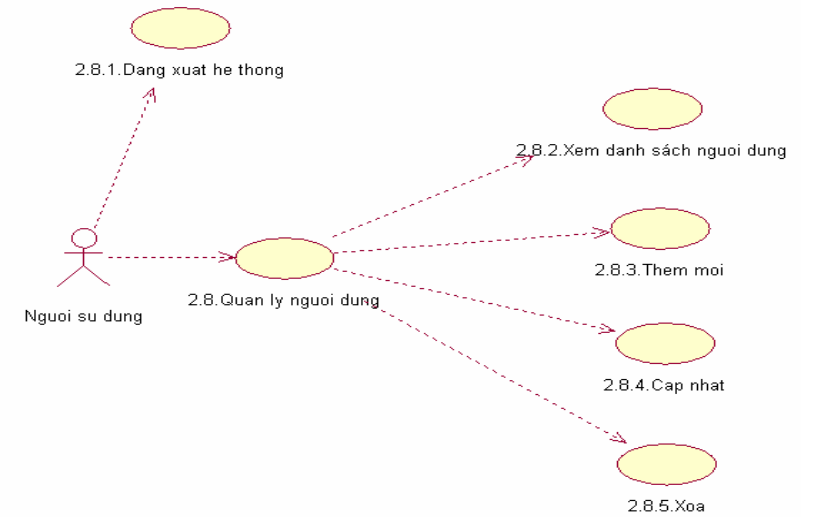
Hình 3.3: *Biểu đồ ca sử dụng quản lý dự án đã làm*

- Biểu đồ ca sử dụng 2.7. Quản lý tài liệu



Hình 3.4: *Biểu đồ ca sử dụng quản lý tài liệu*

- Biểu đồ ca sử dụng 2.8. Quản lý người dùng



Hình 3.5: *Biểu đồ ca sử dụng quản lý người dùng*

3.4. THỰC HIỆN CÁC CA KIỂM THỬ

Sau khi có được danh sách các yêu cầu và biểu đồ ca sử dụng, chúng tôi sẽ tiến hành thực thi kiểm thử website LAT. Trong phần thực thi kiểm thử này chúng tôi tiến hành thực thi kiểm thử theo hai phương pháp kiểm thử. Phương pháp thứ nhất là thực hiện thủ công, phương pháp này chủ yếu sẽ kiểm thử các chức năng của website LAT. Phương pháp thứ hai là thực thi kiểm thử bảo mật bằng công cụ ***"Acunetix Web Vulnerability Scanner"*** , phương pháp này sẽ tập trung vào kiểm thử các lỗi bảo mật của website LAT.

3.4.1. Thực hiện kiểm thử thủ công

3.4.2. Thực hiện kiểm thử bằng công cụ Acunetix Web Vulnerability Scanner

3.5. ĐÁNH GIÁ VỀ MỨC ĐỘ BẢO MẬT WEBSITE WWW.LAT.COM.VN

3.5.1. Kết quả kiểm thử thủ công

Bảng 3.6: *Bảng đánh giá kết quả thủ công*

TT	Tên chức năng	Số ca kiểm thực thi	Số ca kiểm thử thành công	Số ca kiểm thử chưa thành công	Tỷ lệ thành công
1	Đăng nhập	4	3	1	**75%**
2	Dự án đã làm	23	13	10	**57%**
3	Tài liệu	15	10	5	**67%**
4	Người dùng	14	7	7	**50%**
- **Tổng trường hợp kiểm thử thực thi : 56**					
- **Tổng số trường hợp thành công : 33**					
- **Tổng số trường hợp thất bại : 23**					
✦ **Kết luận chung kết quả kiểm thử thủ công** - Qua số liệu các ca kiểm thử thành công và thất bại ở trên ta có thể thấy được tỷ lệ các ca kiểm thử thành công chiếm 59 %, tỷ lệ các kiểm thử thất bại là 41 %. - Tỷ lệ ca kiểm thử thất bại là 41% cũng đồng nghĩa với việc tỷ lệ lỗi sau khi quét bằng tay là 41%, đây là tỷ lệ lỗi lớn.					

3.5.2. Kết quả kiểm thử tự động

Bảng 3.7: *Bảng đánh giá kết quả tự động*

TT	Loại lỗi bảo mật	Số cảnh báo	Mô tả lỗi	Mức độ nghiêm trọng
1	Dùng phiên bản PHP cũ	1	Đây là lỗi sử dụng ngôn ngữ lập trình cũ hơn so với hiện tại. Vì là phiên bản cũ nên còn tồn tại một số lỗi và điều này dẫn đến website dễ bị tấn công.	**Cao**
2	Dùng phiên bản máy chủ web Apache phiên bản cũ	1	Đây là lỗi sử dụng máy chủ web apche phiên bản cũ. Phiên bản cũ còn tồn tại nhiều lỗi bảo mật, dẫn đến website dễ bị tấn công	**Trung bình**
3	PHP allow_url_fopen enabled	1	Lỗi cho phép thêm các đoạn mã trên trình duyệt, gây nguy cơ bị tấn công bằng xss hoặc sqlInjection	**Cao**
4	PHP errors enabled	1	Lỗi này cho phép hiển thị các lỗi lên trình duyệt. Lỗi này dễ bị các kẻ tấn công lợi dụng câu thông báo lỗi để biết website viết bằng ngôn ngữ gì, máy chủ là gì, phiên bản bao nhiêu… và từ đó khai thác các lỗi bảo mật.	**Trung bình**
5	MySQL Server weak password	1	Đây là lỗi mật khẩu của hệ quản trị cơ sở dữ liệu MySQL có mức độ bảo mật yếu. Dẫn đến mật khẩu dễ bị đoán và dễ bị tấn công chiếm quyền kiểm soát cơ sở dữ liệu	**Cao**
6	File inputs accepted	12	Lỗi này cho phép người dùng có thể thực hiện tải tất cả các tập tin lên máy chủ. Điều này	**Thấp**

TT	Loại lỗi bảo mật	Số cảnh báo	Mô tả lỗi	Mức độ nghiêm trọng
			dễ bị các kẻ tấn lợi dụng để tại các tập tin chứa những đoạn mã độc hại.	
7	TRACE Method Enabled		Lỗi này cho phép kẻ tấn công có thể thay đổi các thông tin về session, cookies, và các dữ liệu về quyền truy cập. Lỗi này thương dùng để tấn công XSS.	**Thấp**

✦ **Kết luận chung kết quả kiểm thử tự động**

- Qua số liệu thống kê lỗi bảo mật cùng những cảnh báo liên quan đến các lỗi bảo mật đó, chúng ta dễ dàng nhận thây được website Lat còn mắc nhiều lỗi bảo mật nghiêm trọng.

- Những lỗi bảo mật này cần được khắc phục kịp thời, nếu không website Lat rất dễ bị tấn công.

KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Kiểm thử bảo mật nói chung và kiểm thử bảo mật website nói riêng luôn là vấn đề cấp thiết và cần được giải quyết triệt để. Ngày nay, khi ngành công nghệ thông tin phát triển với một tốc độ chóng mặt thì vấn đề về kiểm thử bảo mật càng trở nên cấp thiết hơn và khó khăn hơn. Điều này thể hiện rõ ràng qua con số thống kê về số lượng website thương mại điện tử kẻ tấn công tấn công mỗi ngày một tăng lên, quy mô các cuộc tấn công và mức độ thiệt hại ngày càng lớn hơn. Trước tình hình thực tế đó, đề tài ***"Nghiên cứu kiểm thử bảo mật website"*** đã được chúng tôi chọn và trình bày làm luận văn thạc sĩ, với hy vọng đóng góp một phần vào việc giải quyết vấn đề về bảo mật.

Sau khi hoàn thành, luận văn đã đạt được một số kết quả như sau: Xét về mặt lý thuyết, luận văn đã đưa ra được tình hình về bảo mật hiện nay dựa trên thống kê của các trang bảo mật nổi tiếng cả của Việt Nam và cả của nước ngoài. Bên cạnh đó luận văn cũng đã giới thiệu được phương thức tấn công, mức độ nguy hiểm cũng như một số giải pháp nhằm hạn chế sự thiệt hại của các kiểu tấn công bảo mật phổ biến hiện nay. Luận văn cũng đưa ra được một số công cụ hỗ trợ trong việc dò tìm các lỗi bảo mật, đã nêu ra quy trình kiểm thử thủ công. Xét về mặt thực tiễn, luận văn đã đưa ra được quy trình kiểm thử cải tiến và chuyên dùng cho việc kiểm thử bảo mật website. Giúp cho các nhà phát triển web an tâm hơn về chất lượng của sản phẩm sau khi được kiểm tra. Và một ý nghĩa thực tiễn khác là đã áp dụng thành công quy trình kiểm thử bảo mật cải tiến kết hợp với

công cụ Acunetix Web Vulnerability Scanner vào kiểm thử bảo mật website lat.com.vn.

Tuy nhiên bên cạnh những điều đạt được, luận văn còn tồn tại một vài điểm hạn chế sau: Hạn chế đầu tiên của luân văn là, những lỗi bảo mật mà đề tài nêu ra chỉ là những lỗi bảo mật phổ biến chứ chưa bao phủ được hết toàn bộ các lỗi bảo mật hiện nay. Hạn chế thứ hai của luận văn chính là về phương pháp kiểm thử mà luận văn. Luận văn nghiên cứu kiểm thử bảo mật web dựa trên mô hình kiểm thử hộp đen là chủ yếu, chưa vận dụng các điểm mạnh của các kỹ thuật kiểm thử khác như kỹ thuật kiểm thử hộp trắng, kỹ thuật kiểm thử hộp xám vào luận văn.

Trên cơ sở nghiên cứu các tư liệu và kết quả thực nghiệm cho thấy kiểm thử bảo mật website là rất quan trọng, việc thực hiện kiểm thử sớm sẽ làm giảm thời gian kiểm thử cho các giai đoạn sau và tăng chất lượng của sản phẩm. Việc thực hiện kiểm thử bảo mật (kiểm thử ngay từ giai đoạn phân tích thiết kệ hệ thống) là rất tốt. Tuy nhiên, để vận dụng và thực hiện một cách hiệu quả các qui trình, phương pháp và công cụ kiểm thử bảo mật vẫn còn nhiều vấn đề đặt ra cần tiếp tục giải quyết. Từ những hạn chế còn tồn đọng của đề tài được trình bày trên. Chúng ta có thể đề xuất những hướng nghiên cứu và triển khai tiếp theo của luận văn là:

- Nghiên cứu thêm một số phương pháp tấn công và cách phòng chống mới nhằm nâng cao hiệu quả trong việc kiểm thử bảo mật website.
- Dựa trên nền tảng kiến thức kiểm thử hộp đen đã có tiến hành xây dựng bộ hồ sơ kiểm thử hộp trắng độ bảo mật của webiste.

- Nghiên cứu thêm về các vấn đề bảo mật, các công cụ mã nguồn mở về dò tìm lỗi bảo mật. Từ đó xây dựng một công cụ hỗ trợ việc dò tìm lỗi bảo mật mới, hoàn thiện hơn, để có thể hỗ trợ tốt hơn vào quy trình kiểm thử bảo mật.