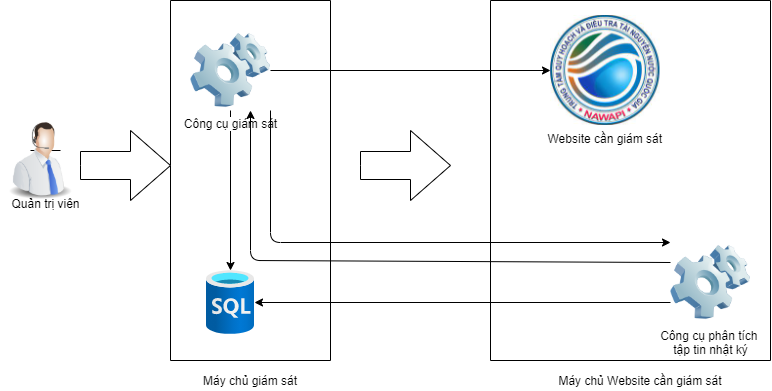
**Tài liệu phân tích thiết kế hệ thống**

1. **Mô hình triển khai**

**

Mô hình các thành phần của bộ công cụ

Mô hình triển khai bao gồm các thành phần chính sau:

**Quản trị viên** thực hiện các thao tác là sử dụng tài khoản đăng nhập vào website giám sát; cấu hình địa chỉ URL cần giám sát và tiếp nhận, xử lý các thông báo từ công cụ giám sát

**Cơ sở dữ liệu** được thiết kế để lưu trữ các thông tin là địa chỉ URL của website cần giám sát, các thông báo từ công cụ giám sát và các thông báo từ công cụ phân tích tập tin

**Công cụ giám sát** là thành phần chính của mô hình, bao gồm 2 cơ chế chính là cơ chế phát hiện thay đổi giao diện và cơ chế xác định và cảnh báo tấn công thay đồi giao diện. Ngoài ra công cụ này sử dụng công nghệ "server send event" để thông báo thời gian thực; sử dụng MySQL làm cơ sở dữ liệu lưu trữ các hình ảnh thu thập, danh sách các URL trang web đang được giám sát cũng như nội dung các cảnh báo tấn công thay đổi giao diện.

**Công cụ phân tích tập tin nhật ký** sẽ tiến hành phân tích tập tin nhật ký ; sau đó gửi kết quả phân tích về cơ sở dữ liệu đồng thời gọi lại cơ chế xác định của công cụ giám sát căn cứ tập luật để xác định và cảnh báo tấn công thay đổi giao diện.

**Website cần giám sát** là các địa chỉ URL được quản trị viên lựa chọn lúc cấu hình công cụ giám sát.

1. **Chức năng của hệ thống**

Bảng thể hiện tổng quát các chức năng của hệ thống

|  |  |  |
| --- | --- | --- |
| **STT** | **Chức năng** | **Mô tả** |
| 1 | Giám sát web | chụp ảnh trang web; lấy và so sánh nội dung, cấu trúc, giao diện, trích xuất và đưa ra hình ảnh sự thay đổi trong bố cục; sử dụng công nghệ "server send event" để thông báo thời gian thực |
| 2 | Phân tích tập tin nhật ký | Đối sánh dòng http request với các biểu thức cấu hình sẵn để phát hiện dấu hiệu tấn công. |

1. **Chi tiết chức năng của hệ thống**

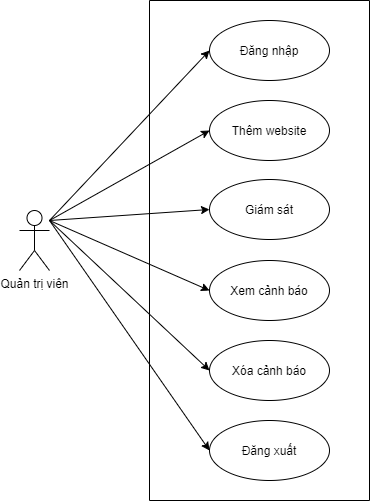
*Giám sát web:* Chụp lại hình ảnh giao diện website

* Đầu vào: Đường link website
* Xử lý: Truy cập website và chụp lại giao diện ở thời điểm truy cập, lấy trích xuất, các đặc trứng, md5, so sánh với các bản lưu trước đó.
* Đầu ra: Thông báo thay đổi giao diện nội dung, thời gian, ảnh minh chứng.

Phân tích tập tin nhật ký:

* Đầu vào: Tập tin nhật ký website
* Xử lý: Đối sánh dòng http request với các biểu thức cấu hình sẵn
* Đầu ra: Dấu hiệu tấn công

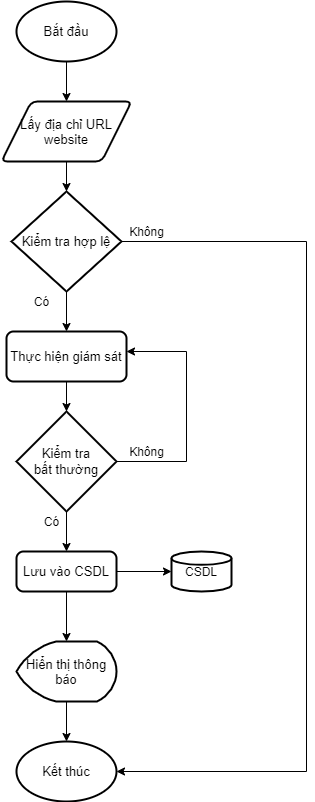
1. **Sơ đồ chức năng của công cụ**
   1. *Chức năng quản trị viên*



*Thiết kế chức năng quản trị viên*

Chức năng Quản trị viên được thiết kế thể hiện gồm giao diện trang đang nhập và trang quản trị. Tại trang đăng nhập, quản trị viên đăng nhập bằng địa chỉ email và mật khẩu được cấu hình sẵn. Sau khi đăng nhập vào trang quản trị, quản trị viên có thể thực hiện các chức năng thêm/ xóa địa chỉ URL của website; xem/ xóa các thông báo về sự thay đổi giao diện; cuối cùng là đăng xuất khỏi phiên làm việc.

* 1. *Chức năng giám sát web*

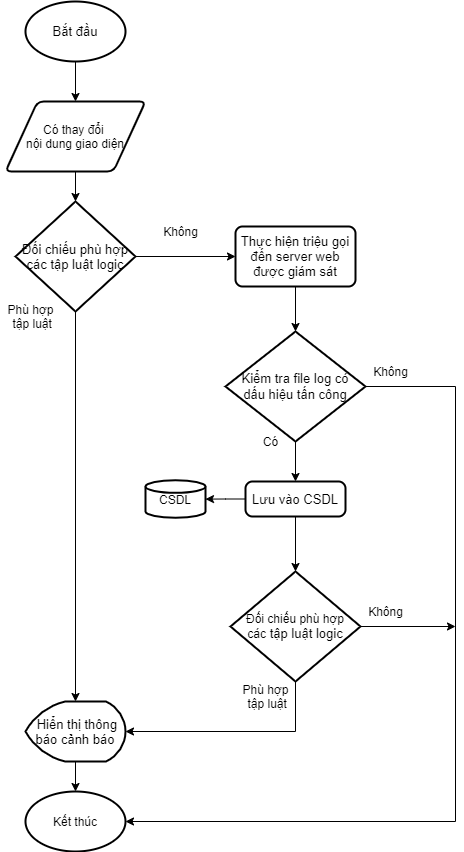


*Thiết kế chức năng giám sát*

Chức năng giám sát thực hiện cơ chế phát hiện thay đổi giao diện theo thời gian lặp liên tục được cấu hình sẵn. Với đầu vào là URL của website, chức năng này tiến hành giám sát website do quản trị viên nhập vào, chụp ảnh và lấy trích xuất cấu trúc, nội dung, thuộc tính của website này; tính checksum MD5 cho hình ảnh, nội dung đã được trích xuất; lưu trữ các thông tin; so sánh và lặt lại nếu không có sự thay đổi; đưa ra thông báo khi có sự khác nhau của style và nội dung so với lần trước của website.

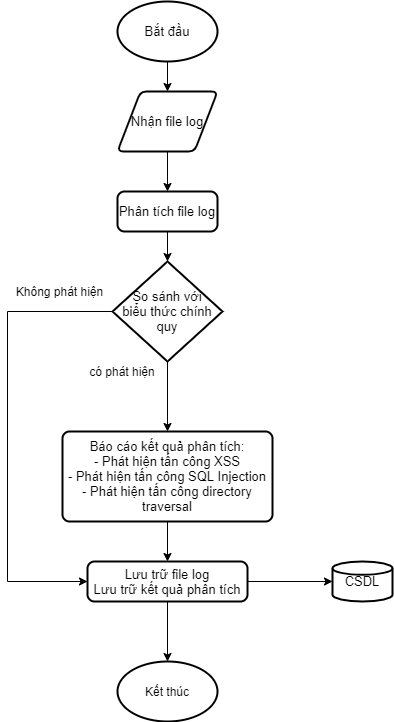
Việc giám sát liên tục này có thể gây nhầm lẫn thành hình thức tấn công từ chối dịch vụ. Để khắc phục nhầm lẫn này, chúng ta có thể cài đặt sự cho phép đối với IP của máy chủ đặt website giám sát trên máy chủ website được giám sát.

* 1. *Thiết kế chức năng xác định tấn công thay đổi giao diện*

**

*Thiết kế chức năng xác định tấn công thay đổi giao diện*

Chức năng xác định tấn công thay đổi giao diện được thiết kế sẽ được gọi đến khi có sự thay đổi giao diện. Đầu vào trường hợp thay đổi nội dung giao diện, chức năng này có nhiệm vụ xác định thay đổi có phải tấn công thay đổi giao diện hay không bằng cách so sánh với các tập luật logic đã phân tích; khi chưa đủ dữ kiện thì tiến hành phân tích tập tin nhật ký và kết hợp kết quả phân tích tập tin nhật ký cùng kết quả trường hợp bị thay đổi để xác định thay đổi có phải tấn công thay đổi giao diện hay không.

**

*Hoạt động của công cụ phân tích tập tin nhật ký*

Hoạt động của công cụ phân tích tập tin nhật ký sẽ đặt tại chính máy chủ website được giám sát. Công cụ sẽ được triệu gọi khi xác định chưa đủ dữ kiện về sự thay đổi có phải là tấn công hay không. Công cụ sẽ tiến hành đọc các dòng của tập tin nhật ký, so sánh với biểu thức cho sẵn để phát hiện ra một số dấu hiện dò quét, tấn công phổ biến như XSS, SQL Injection cũng như nguồn truy cập điều khiển không hợp lệ. Sau đó hoạt động này trả kết quả về máy chủ website giám sát để ra quyết định.