Defacements-monitering

NGUYỄN ANH TUẤN - CB180204 –

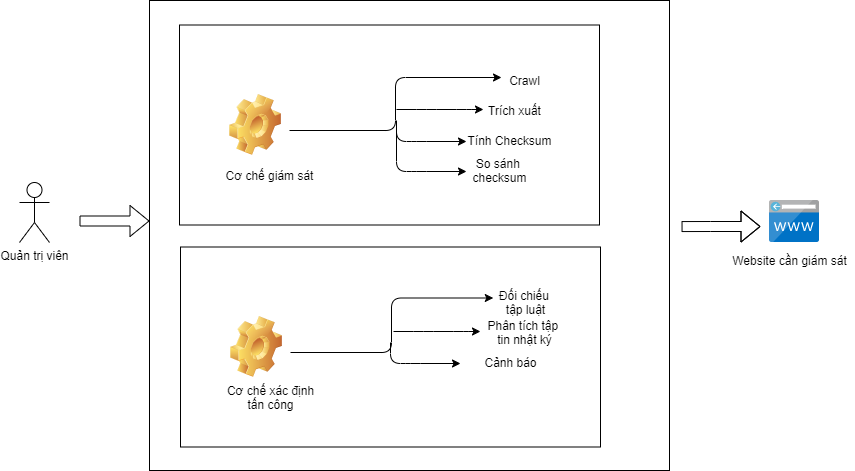
Đề tài Thạc sĩ : Phát hiện tấn công websites defacements

* Hướng tiếp cận
* Mô hình giải pháp và triển khai
* Môi trường, công cụ sử dụng
* Cài đặt môi trường
* Cấu hình mã nguồn

Hướng tiếp cận

Xây dựng công cụ giám sát sự thay đổi nội dung website, có khả năng phát hiện và đưa ra cảnh báo các trường hợp website bị thay đổi nội dung, giao diện hay chèn các đoạn mã có khả năng gây hại. Trên máy chủ có kết nối đến website cần giám sát, triển khai một phần mềm liên tục giám sát nội dung website, ghi nhận và so sánh các trường hợp website có sự thay đổi về giao diện, nội dung, đưa ra cảnh báo theo thời gian thực kèm theo hình ảnh minh chứng cho sự thay đổi. Người quản trị dựa trên các cảnh báo mà công cụ đưa ra, kiểm tra các vị trí khả nghi có thể liên quan đến tấn công thay đổi giao diện để kịp thời khắc phục sự cố (nếu có).

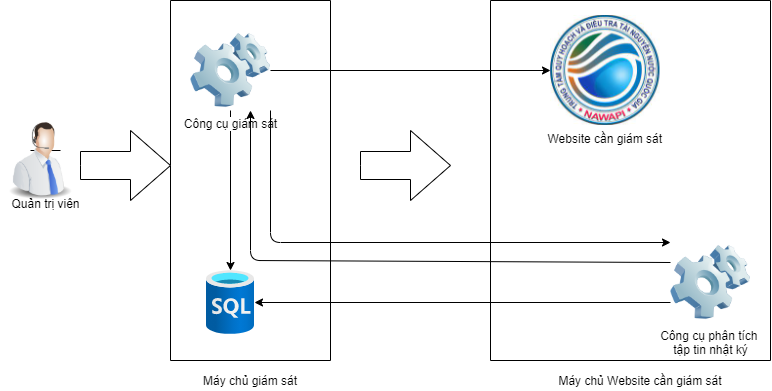
## Mô hình giải pháp

**

Mô hình giải pháp đề xuất 02 cơ chế:

* Cơ chế giám sát
* Cơ chế xác định tấn công

**Mô hình triển khai**

**

Mô hình triển khai bao gồm các thành phần

* + Quản trị viên
  + Công cụ giám sát
  + Cơ sở dữ liệu
  + Công cụ phân tích tập tin nhật ký
  + Website cần giám sát

Mô trường, công cụ sử dụng

* hệ điều hành Windows 10
* XAMPP
* NodeJS
* Website NAWAPI, đã cấu hình dịch vụ phân giải tên miền DNS tại địa chỉ: http://forecasting.vaci.org.vn/, được cài đặt trên giải IP nội bộ là http://10.1.101.72/cbdb/public
* Hệ thống hỗ trợ và quản lý biên bản cuộc họp tại UBND thành phố Hà Nội, đã được cấu hình dịch vụ phân giải tên miền DNS tại địa chỉ: https://tiepcancntt.com:8888/, Được cài đặt trên máy chủ localhost để thử nghiệm là http://localhost/tiepcancntt
* Công cụ giám sát (Web monitoring) hoạt động trên giao diện web theo địa chỉ: http://localhost:3000. Tài khoản quản trị viên sử dụng để đăng nhập là: natuan9@monre.gov.vn /123456.

**Cài đặt môi trường**

1. Cài đặt máy chủ Apache

Download Xampp source từ địa chỉ http://apachefriends.org phiên bản 64 bit hoặc 32 bit. Sau đó cài đặt trên windows bao gồm cả Apache và MySQL.

1. Cài đặt NodeJS

Bước 1: Download NodeJS

Để download NodeJS cần truy cập vào địa chỉ dưới đây:

<https://nodejs.org/en/download/> sau đó lựa chọn phiên bản phù hợp với Hệ điều hành (32 bit hoặc 64 bit) để tải về.

Bước 2- Cài đặt NodeJS

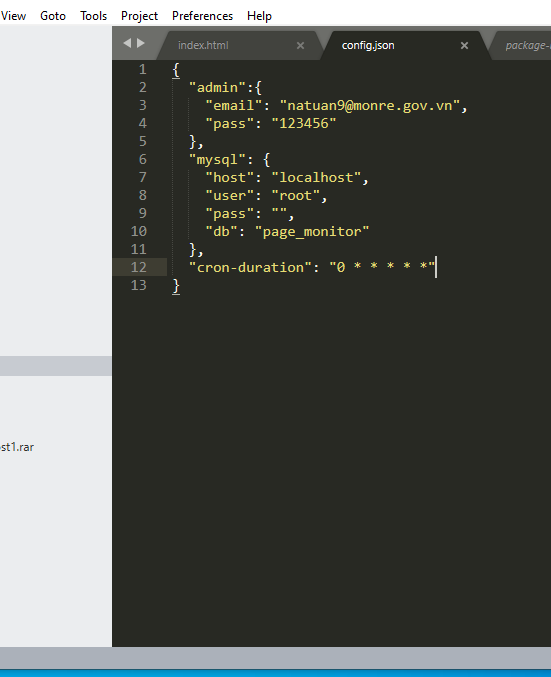
Cài đặt NodeJS trên Windows rất đơn giản, chấp nhận các tùy chọn mặc định và nhấn "Next .. Next" cho tới bước cuối cùng.

Theo mặc định, phần mềm NPM cũng được cài đặt vào hệ thống. Đây là một phần mềm quản lý các thư viện Javascript.

**Cấu hình mã nguồn**

Bước 1: đăng nhập vào phpmyadmin, tạo cơ sở dữ liệu tên 'page\_monitor', import tệp tin 'setting.sql' vào cơ sở dữ liệu vừa tạo

Bước 2: mở tệp tin config.json tạo tài khoản quản trị và điền tài khoản đăng nhập cơ sở dữ liệu



*Cấu hình mã nguồn công cụ*

**Khởi tạo phiên làm việc**

1. Khởi tạo môi trường

Bước 1: Khởi chạy XAMPP , bật start cho Apache, MySQL

Bước 2: Khởi chạy file Start\_monitor.bat

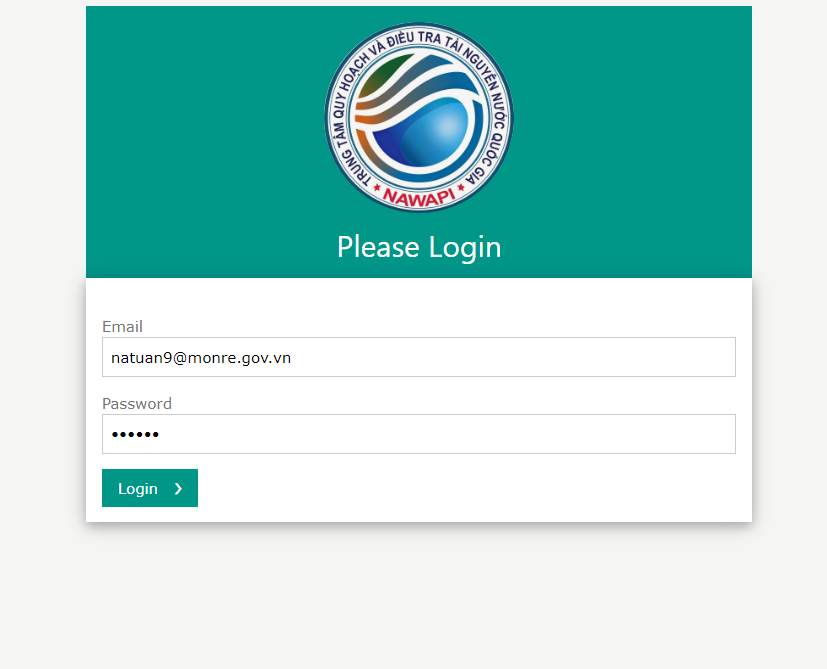
1. Khởi tạo phiên làm việc

Bước 1: Trên máy tính 1 tiến hành chạy dịch vụ giám sát.



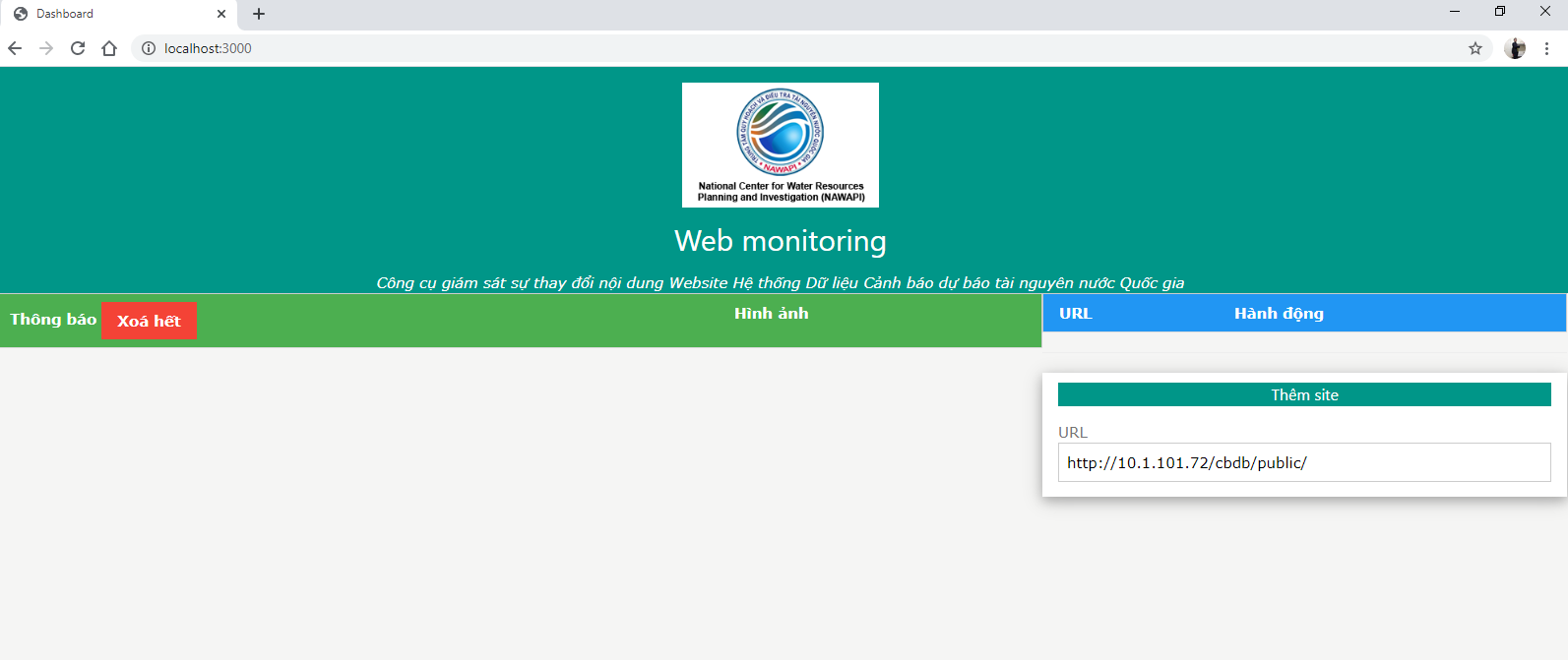
*Khởi chạy dịch vụ giám sát*

Bước 2: Đăng nhập vào website quản trị tại địa chỉ http://localhost:3000



Đăng nhập vào website quản trị

Bước 3: Thêm địa chỉ URL của website cần giám sát



*Thêm địa chỉ URL của Website cần giám sát*

Bước 4: Theo dõi thông báo xuất hiện tại trang quản trị



*Thông báo xuất hiện tại trang quản trị*