TRƯỜNG ĐẠI HỌC THĂNG LONG

**KHOA CÔNG NGHỆ THÔNG TIN**

****

**BÀI TẬP LỚN**

**ĐỀ TÀI: Khám phá và bảo vệ chống lại các lỗ hổng bảo mật trong hệ thống quản lý nội dung (CMS) WordPress**

|  |  |
| --- | --- |
| **Giáo viên hướng dẫn:** | **Thành viên nhóm:** |
| Nguyễn Hữu Tiến | A41798 – Đỗ Quỳnh Thi |
|  | A41791 - Ninh Thị Thanh |

**HÀ NỘI – 2024**

**MỤC LỤC**

[Chương 1. Tổng quan hệ thống 3](#_Toc176720141)

[1.1. Hệ thống quản lý nội dung (CMS) 3](#_Toc176720142)

[1.1.1. Định nghĩa 3](#_Toc176720143)

[1.1.2. Chức năng 3](#_Toc176720144)

[1.1.3. Phân loại 4](#_Toc176720145)

[1.1.4. Lợi ích 5](#_Toc176720146)

[1.1.5. Một số hệ thống phổ biến 6](#_Toc176720147)

[1.2. WordPress 8](#_Toc176720148)

[1.2.1. Giới thiệu về WordPress 8](#_Toc176720149)

[1.2.2. Phân loại WordPress: 9](#_Toc176720150)

[1.2.3. Các thành phần chính của WordPress 10](#_Toc176720151)

[1.2.4. Cách thức hoạt động của WordPress 13](#_Toc176720152)

[1.2.5. Ưu điểm và nhược điểm của WordPress 14](#_Toc176720153)

[Chương 2. Lỗ hổng bảo mật và cách phòng chống 16](#_Toc176720154)

[2.1. Lỗ Hổng Brute Force 16](#_Toc176720155)

[2.2. SQL Injection 17](#_Toc176720156)

[2.3. Phần mềm độc hại 19](#_Toc176720157)

[2.4. Cross-Site Scripting - XXS 20](#_Toc176720158)

[2.5. Dịch vụ từ chối phân tán (DDoS) 22](#_Toc176720159)

[2.6. Cross-Site Request Forgery (CSRF) 23](#_Toc176720160)

[Chương 3. Demo 25](#_Toc176720161)

[3.1. Công cụ WPScan và Metasploit Framework 25](#_Toc176720162)

[3.1.1. WPScan 25](#_Toc176720163)

[3.1.2. Metasploit framework 25](#_Toc176720164)

[3.2. Tấn công Wordpress 26](#_Toc176720165)

[3.2.1. Tấn công qua lỗ hổng SQL Injection 26](#_Toc176720166)

[3.2.2. Tấn công brute force 27](#_Toc176720167)

[3.2.3. Tấn công qua lỗ hổng version Wordpress 29](#_Toc176720168)

# Tổng quan hệ thống

## Hệ thống quản lý nội dung (CMS)

### Định nghĩa

Hệ thống quản lý nội dung CMS (viết tắt của Content Management System) là một hệ thống được sử dụng để quản lý, tạo ra và điều chỉnh nội dung trên các trang web một cách hiệu quả và dễ dàng. Các loại nội dung bao gồm văn bản, hình ảnh, video, bài viết blog, sản phẩm trong trường hợp của trang thương mại điện tử, và nhiều loại nội dung khác.Hệ thống CMS sẽ giúp bạn tuỳ chỉnh thiết kế, chức năng của website của mình bằng cách tải xuống hoặc mua các mẫu thiết kế có sẵn.

Các hệ thống thông tin quản lý CMS được xem như “trung tâm đầu não” của một website, giúp quản lý hầu hết các nội dung mà doanh nghiệp cho đăng tải trên website của mình. Hiện nay, CMS được sử dụng rộng rãi tại các doanh nghiệp lớn, tổ chức và các cá nhân, nhờ tính tiện lợi, dễ sử dụng, tiết kiệm thời gian, chi phí xây dựng và vận hành một website chuyên nghiệp.

A diagram of a content management system

Description automatically generated

### Chức năng

* **Quản lý người dùng:** CMS cho phép tạo và quản lý tài khoản người dùng với các cấp độ truy cập và quyền khác nhau.
* **Tạo và chỉnh sửa nội dung:**CMS cung cấp nhiều công cụ để tạo, chỉnh sửa, và xuất bản nhanh chóng các loại nội dung kỹ thuật số như văn bản, hình ảnh, và video.
* **Kiểm soát phiên bản:**  khả năng theo dõi và quản lý các thay đổi trên nội dung của mình. Điều này giúp dễ dàng quay lại phiên bản trước nếu cần.
* **Mẫu và chủ đề:** CMS cung cấp các mẫu và chủ đề thiết kế sẵn, giúp nhanh chóng tạo ra giao diện nhất quán cho trang web hoặc sản phẩm.
* **Quản lý phương tiện:** dễ dàng quản lý và sắp xếp các nội dung phương tiện kỹ thuật số như hình ảnh và video thông qua CMS.
* **Chức năng tìm kiếm:** CMS hỗ trợ công cụ tìm kiếm và lọc nội dung, giúp dễ dàng định vị và quản lý nội dung khi cần thiết.

### Phân loại

Với sự phát triển nhanh chóng của công nghệ và các yêu cầu khác nhau từ người dùng, CMS đã được phân loại theo nhiều tiêu chí khác nhau.

**1. Phân loại CMS dựa trên nền tảng triển khai**

* **CMS dựa trên Web (W-CMS):**
  + **Đặc điểm:** Đây là loại CMS phổ biến nhất, sử dụng để quản lý nội dung trên các trang web. Hệ thống này hỗ trợ người dùng tạo và quản lý nội dung một cách trực quan thông qua giao diện web.
  + **Ví dụ:** WordPress, Drupal, Joomla, Wix.
* **CMS Dựa Trên Đám Mây (Cloud-Based CMS):**
  + **Đặc điểm:** Được triển khai và lưu trữ trên các máy chủ đám mây, cho phép truy cập từ bất kỳ đâu có kết nối Internet.
  + **Ví dụ:** Contentful, Prismic, Sanity.

**2. Phân Loại CMS dựa trên nguồn gốc mã nguồn**

* **CMS mã nguồn mở (Open Source CMS):**
  + **Đặc điểm:** là phần mềm có mã nguồn mở được cung cấp miễn phí bởi các tập đoàn công nghệ lớn. Người dùng có thể tùy chỉnh và mở rộng các chức năng bằng các plugin
  + **Ví dụ:** WordPress, Joomla, Drupal.
* **CMS tự xây dựng hoặc dùng Framework:**
  + **Tự xây dựng:** Nhà phát triển tự tạo ra một CMS hoàn toàn mới từ đầu, phù hợp với các yêu cầu đặc thù của dự án.
  + **Sử dụng Framework:** Nhà phát triển tận dụng các thư viện và công cụ có sẵn từ các framework để xây dựng CMS, giúp tiết kiệm thời gian nhưng có thể giới hạn trong việc tùy chỉnh.
  + **Ví dụ:** Các CMS phát triển trên nền tảng Laravel, Symfony.
* **CMS mất phí:**
  + **Đặc điểm:** là loại phần mềm CMS được cung cấp từ các đơn vị sản xuất, kinh doanh CMS. Phải trả phí để sử dụng và không thể tùy chỉnh sâu.
  + **Ví dụ:** Squarespace, Shopify,..

**3. Phân Loại CMS Dựa Trên Lĩnh Vực Sử Dụng**

* **Web CMS (W-CMS):** Hệ thống quản lý nội dung chủ yếu cho các trang web, giúp người dùng quản lý và cập nhật nội dung trực tuyến.
* **Enterprise CMS (E-CMS):** Hệ thống quản lý nội dung dành cho các doanh nghiệp lớn, tích hợp nhiều tính năng phục vụ quản lý nội dung trên quy mô toàn doanh nghiệp.
* **Transactional CMS (T-CMS):** Hệ thống hỗ trợ quản lý các giao dịch thương mại điện tử, như giỏ hàng, thanh toán, và các giao dịch trực tuyến.
* **Publications CMS (P-CMS):** Hệ thống quản lý nội dung chuyên phục vụ việc quản lý và xuất bản các ấn phẩm trực tuyến như sách, tạp chí, hướng dẫn và tài liệu tham khảo.
* **Learning CMS (L-CMS/LCMS):** Hệ thống quản lý nội dung hỗ trợ quản lý các chương trình đào tạo trực tuyến, phục vụ cho việc học tập và giáo dục trên nền web.
* **Billing CMS (BCMS):** Hệ thống quản lý nội dung hỗ trợ việc quản lý thu chi, hóa đơn và các giao dịch tài chính trên nền web.

### Lợi ích

* **Tối ưu thời gian và chi phí**
* Tùy vào nhu cầu sử dụng, có thể chọn các hệ thống CMS miễn phí hoặc tự xây dựng với giá rẻ hơn so với xây dựng website bình thường.
* Giảm thiểu chi phí nhân sự: Việc quản lý website trở nên đơn giản hơn, cần ít nhân sự để quản trị và triển khai.
* **Tăng tính linh hoạt**
* Tùy chỉnh giao diện: CMS cho phép bạn tùy chỉnh giao diện website theo ý muốn, từ màu sắc, bố cục đến các tính năng.
* Mở rộng chức năng: Với hệ thống plugin và module đa dạng, bạn có thể bổ sung thêm nhiều chức năng mới cho website của mình.
* Tích hợp với các dịch vụ khác: CMS dễ dàng tích hợp với các dịch vụ bên thứ ba như Google Analytics, Facebook Pixel, email marketing,...’
* **Tương thích trên nhiều thiết bị**
* Responsive design: Hầu hết các CMS hiện nay đều hỗ trợ responsive design, giúp website hiển thị tốt cả trên các thiết bị di động.
* **Dễ dàng quản lý**
* Hệ thống để hỗ trợ việc phân quyền, chia sẻ quyền hạn cập nhật nội dung website cho các nhân viên liên quan giúp quản lý lượng lớn dữ liệu.
* Giao diện trực quan, không cần lập trình.

### Một số hệ thống phổ biến

1. **CMS WordPress**

* Là một hệ thống quản lý nội dung mã nguồn mở thường dùng để xây dựng blog cá nhân hoặc trang tin tức, thương mại điện tử.
* Hệ thống này cho phép người dùng có thể tạo, chỉnh sửa những nội dung, tùy chính và mở rộng đấy dễ dàng mà không cần biết đến code.
* Không cần trả phí

1. **CMS Joomla**

* Là một hệ thống quản lý nội dung mã nguồn mở, phù hợp với dự án doanh nghiệp lớn hoặc tổ chức với nhu cầu tùy chỉnh cao, quản lý nội dung phức tạp.
* Cách sử dụng hệ thống này tương đối khó và phức tạp
* Không cần trả phí

1. **CMS Drupal**

* Là một hệ thống quản lý nội dung mã nguồn mở, thường được sử dụng trong các doanh nghiệp lớn với nhu cầu tùy biến và bảo mật cao.
* Hệ thống này hơi khó để điều chỉnh giao diện website khi cần thiết.
* Không cần trả phí

1. **CMS Magento**

* Là một hệ thống quản lý nội dung mã nguồn mở được thiết kế đặc biệt để xây dựng và quản lý các trang web thương mại điện tử phù hợp với doanh nghiệp kinh doanh trực tuyến.
* Có phiên bản miễn phí và trả phí

1. **CMS Opencart**

* Là một hệ thống quản lý nội dung mã nguồn mở được thiết kế đặc biệt để xây dựng và quản lý các cửa hàng trực tuyến.
* Tính năng đặc biệt là Multishop, có nghĩa là có thể tạo được nhiều cửa hàng trên một website.
* Dễ dính lỗi, các module còn chưa được linh hoạt

1. **CMS Typo3**

* Là một hệ thống quản lý nội dung mã nguồn mở, chạy được trên nhiều hệ điều hành
* Không có theme có sẵn
* Không cần trả phí

1. **CMS Shopify**

* Là một nền tảng CMS lưu trữ tất cả trong một, phù hợp với cửa hàng thực và trực tuyến
* Chi phí cao

1. **CMS Squarespace**

* Là một hệ thống quản lý nội dung (CMS) tích hợp được thiết kế để xây dựng và quản lý các trang web và cửa hàng trực tuyến.
* Cung cấp khả năng tối ưu SEO
* Thiếu tính năng tự động lưu khi chỉnh sửa, không có tùy chọn cho các plugin.

1. **CMS Wix**

* Là một nền tảng xây dựng trang web dựa trên trình chỉnh sửa kéo và thả (drag-and-drop).
* Nếu muốn phát triển cửa hàng E-commerce thì phải nâng cấp lên gói trả phí.

1. **CMS Ghost**

* Là một hệ thống quản lý nội dung (CMS) mã nguồn mở,tập trung vào việc cung cấp một giao diện đơn giản và trải nghiệm viết bài tập trung cho các nhà văn và blogger.
* Không hỗ trợ cài đặt plugin từ bên thứ ba

## WordPress

### Giới thiệu về WordPress

WordPress là một hệ thống mã nguồn mở dùng để xuất bản blog/website được viết bằng ngôn ngữ lập trình PHP và cơ sở dữ liệu MySQL. WordPress được biết đến như một CMS miễn phí nhưng tốt, dễ sử dụng và phổ biến nhất trên thế giới.

* **Lịch sử hình thành**
* WordPress là sự kế thừa chính thức từ một công cụ viết blog được phát triển bởi lập trình viên người Pháp Michel Valdrighi có tên là b2/cafelog, ra mắt lần đầu tiên vào năm 2001.
* Đến ngày 27 tháng 5 năm 2003, WordPress mới chính thức được phát hành phiên bản đầu tiên bởi Matt Mullenweg và Mike Little.
* Hiện nay, WordPress chiếm khoảng 43% tổng số website trên toàn thế giới, trở thành một trong những CMS phổ biến và lâu đời nhất.
* **Một số loại website được tạo từ WordPress**
* Blog cá nhân
* Website doanh nghiệp
* Cửa hàng trực tuyến
* Trang tin tức
* Diễn đàn
* Portfolio
* Website giáo dục
* Website phi lợi nhuận
* Website cộng đồng
* Website phổ biến dùng Wordpress

1. Coca Cola France

2. Sony Music

3. Vogue Magazine

4. CNN Press Room

5. BBC America

6. Forbes

7. Blog MTV News

8. LinkedIn Blog

9. SAP News Center

10. The Harvard Gazette

A close-up of a computer

Description automatically generated

### Phân loại WordPress:

| **Đặc điểm** | **WordPress.com** | **WordPress.org** |
| --- | --- | --- |
| **Hosting** | Được cung cấp bởi WordPress.com | Bạn tự quản lý hosting hoặc sử dụng dịch vụ hosting của bên thứ ba |
| **Cài đặt và quản lý** | Không cần tự cài đặt, chỉ cần đăng ký tài khoản và bắt đầu sử dụng | Bạn phải tự cài đặt WordPress trên máy chủ của mình và tự quản lý |
| **Tùy chỉnh** | Giới hạn về tùy chỉnh, không thể truy cập vào mã nguồn của trang web | Hoàn toàn có thể tùy chỉnh và truy cập vào mã nguồn của trang web |
| **Plugin và chủ đề** | Giới hạn trong việc cài đặt plugin và chủ đề, chỉ có thể sử dụng các plugin và chủ đề được phê duyệt bởi WordPress.com | Có thể cài đặt và sử dụng bất kỳ plugin và chủ đề nào mà bạn muốn |
| **Quảng cáo** | WordPress.com có thể hiển thị quảng cáo trên trang web của bạn, nếu bạn không nâng cấp lên gói trả phí | Không có quảng cáo được hiển thị mặc định |
| **Kiểm soát và tự do** | Kiểm soát và tự do ít hơn về việc quản lý và tùy chỉnh trang web | Có kiểm soát và tự do tối đa về quản lý và tùy chỉnh trang web |
| **Phí** | Có các gói trả phí với các tính năng mở rộng, như loại bỏ quảng cáo, tên miền tùy chỉnh và lưu trữ nâng cao | WordPress.org là miễn phí, bạn chỉ phải trả phí cho tên miền và hosting (nếu áp dụng) |

Bảng 1.1.Phân loại WordPress

Tóm lại, WordPress.com thích hợp cho những người muốn một giải pháp dễ dàng và không cần kiến thức kỹ thuật nhiều, trong khi WordPress.org phù hợp cho những người muốn có sự linh hoạt và kiểm soát cao nhất đối với trang web của mình. Trong bài báo cáo này tập trung phân tích và tìm hiểu về WordPress.org.

### Các thành phần chính của WordPress

WordPress là một hệ thống quản lý nội dung (CMS) phổ biến, với các thành phần chính bao gồm:

1. **WordPress Core**

* **Định nghĩa**: Đây là bộ khung nền tảng chính của WordPress, cung cấp các chức năng cốt lõi như quản lý bài viết, trang, bình luận, người dùng, và cấu hình cơ bản của website.
* **Chức năng:**
* Xử lý các yêu cầu HTTP từ trình duyệt.
* Tương tác với cơ sở dữ liệu để lưu trữ dữ liệu.

1. **Themes (Giao diện)**

* **Định nghĩa:** Theme quyết định giao diện trực quan của website, bao gồm bố cục, màu sắc, phông chữ và các yếu tố thiết kế khác.
* **Chức năng:**
* Hiển thị nội dung theo cách trực quan và hấp dẫn.
* Tùy chỉnh giao diện để phù hợp với từng loại website và thương hiệu.
* Có thể tùy chỉnh sâu hơn bằng cách chỉnh sửa mã nguồn.

1. **Plugins (Tiện ích mở rộng)**

* **Định nghĩa:** Plugin là các phần mềm nhỏ được thêm vào WordPress để mở rộng chức năng của website.
* **Chức năng:**
* Thêm các tính năng mới như:
* Tối ưu hóa SEO
* Tạo form liên hệ
* Thêm cửa hàng trực tuyến
* Bảo mật
* ….
* Tích hợp với các dịch vụ bên thứ ba..

1. **Database (Cơ sở dữ liệu)**

* **Định nghĩa:** WordPress sử dụng cơ sở dữ liệu (thường là MySQL) để lưu trữ tất cả dữ liệu của website như bài viết, trang, bình luận, cài đặt, và thông tin người dùng.
* **Chức năng:**
* Lưu trữ dữ liệu một cách có cấu trúc.
* Cho phép truy xuất và cập nhật dữ liệu một cách hiệu quả.

1. **Admin Dashboard :**

* **Định nghĩa:** Admin Dashboard là giao diện quản trị của WordPress, là trung tâm điều khiển, cung cấp cho cái nhìn tổng quan về tình trạng website, các công cụ để thực hiện các tác vụ quản trị và tùy chỉnh website theo ý muốn.
* **Chức năng:**
* ***Quản lý nội dung*:** Admin Dashboard cung cấp các công cụ để tạo, chỉnh sửa, xóa bài viết, trang, quản lý phương tiện (media), và kiểm duyệt nhận xét.
* ***Quản lý giao diện:*** Từ Admin Dashboard, người dùng có thể cài đặt, kích hoạt và tùy chỉnh theme (giao diện) của trang web.
* ***Cài đặt và quản lý plugin:*** Người dùng có thể tìm kiếm, cài đặt và cấu hình các plugin để thêm các tính năng mới vào trang web.
* ***Quản lý người dùng***: Admin Dashboard cho phép tạo, xóa, và chỉnh sửa tài khoản người dùng, cũng như phân quyền cho từng vai trò khác nhau.
* ***Cấu hình cài đặt:*** Người dùng có thể điều chỉnh các cài đặt của trang web như tiêu đề, mô tả, URL tĩnh (permalink), định dạng ngày giờ, và ngôn ngữ.
* ***Cập nhật hệ thống:*** Bảng điều khiển hiển thị thông báo về các bản cập nhật của WordPress, theme, và plugin, đồng thời cho phép người dùng thực hiện cập nhật trực tiếp từ dashboard.
* ***Thống kê và báo cáo:*** Admin Dashboard có thể hiển thị các báo cáo và thống kê về lượng truy cập, hiệu suất trang web, và các hoạt động của người dùng.

### Cách thức hoạt động của WordPress

A diagram of a company's workflow

Description automatically generated

Hình 1.1.Cách hoạt động của WordPress

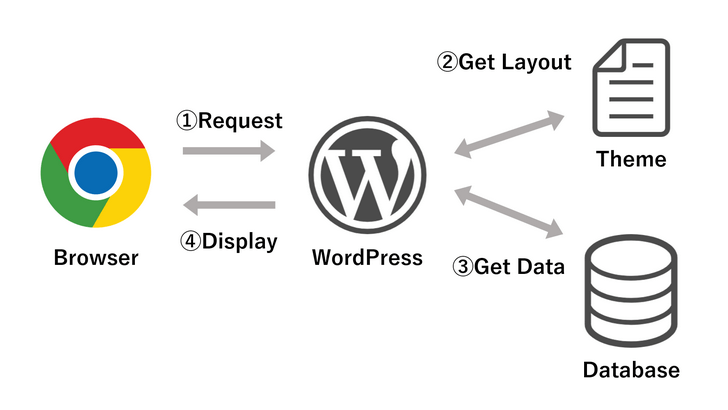
**1. Tạo nội dung:** Người đóng góp nội dung tạo ra nội dung mới và gửi đi phê duyệt.

**2. Phê duyệt nội dung:** Người phê duyệt hoặc biên tập viên kiểm tra và phê duyệt nội dung.

**3. Lưu trữ nội dung:** Nội dung đã được phê duyệt được lưu trữ trên máy chủ của CMS.

**4.Hiển thị website:**

* Khi người dùng truy cập website, máy chủ nhận được yêu cầu và chuyển nó đến WordPress. WordPress sẽ phân tích yêu cầu để xác định bạn muốn xem trang nào.
* Truy xuất thông tin: WordPress truy cập vào cơ sở dữ liệu để lấy ra các thông tin cần thiết
* Tải và áp dụng theme: Sau khi nội dung được truy xuất từ cơ sở dữ liệu, WordPress tải theme đã được kích hoạt. Theme chứa các tệp mẫu (template files) xác định cách thức nội dung được hiển thị trên trang web.
* Kết hợp dữ liệu và thiết kế để tạo ra mã HTML. Sau đó WordPress gửi mã HTML đến trình duyệt.
* Trình duyệt hiển thị nội dung trên màn hình người dùng.



### Ưu điểm và nhược điểm của WordPress

* Ưu điểm
* **Giao diện thân thiện, dễ sử dụng và quản lý:** WordPress được thiết kế với giao diện dễ dàng cho mọi người, kể cả những người không chuyên cũng có thể tạo và quản lý website của mình.
* **Hỗ trợ tối ưu SEO hiệu quả:** Nền tảng WordPress cung cấp nhiều plugin và các công cụ hỗ trợ tối ưu SEO, qua đó giúp nâng cao thứ hạng của website trên các thanh tìm kiếm.
* **Tiết kiệm chi phí hiệu quả:**WordPress có sẵn hàng loạt các giao diện miễn phí, hỗ trợ người dùng tạo một website chuyên nghiệp dễ dàng mà không tốn phí.
* **Tính năng mở rộng và nâng cấp:**Kho WordPress hiện**có hơn 40.000 plugin và theme** (miễn phí và có tính phí), cho phép người dùng mở rộng thêm các tính năng và thiết kế giao diện website theo cách bạn muốn.
* **Tính linh hoạt:**Bên cạnh kho plugin và theme chất lượng, WordPress còn cho phép người dùng tùy chỉnh mọi khía cạnh của website (giao diện, chức năng) một cách dễ dàng qua mã nguồn mở và API.
* **Hỗ trợ đa ngôn ngữ:** Tính đến thời điểm tháng 1/2022, **WordPress đã hỗ trợ hơn 200 ngôn ngữ**. Điều này đồng nghĩa với việc bạn có thể tùy chỉnh cấu hình và hiển thị nội dung website trong hầu hết các ngôn ngữ trên thế giới.
* **Cộng đồng sử dụng và hỗ trợ rộng lớn:** Nhờ vào số lượng các nhà phát triển, thương hiệu và người dùng trên WordPress, dễ dàng tìm kiếm tài liệu, các nguồn tài nguyên và sự hỗ trợ.
* Nhược điểm
* **Tính bảo mật:** Vì là mã nguồn mở và có độ phổ biến rất cao, nên nếu không được lập trình và bảo vệ đúng cách, website có thể dễ dàng bị tấn công bởi các hacker.
* **Hiệu suất trang Web:** Việc cài đặt quá nhiều plugin hoặc template phức tạp có thể ảnh hưởng tới hiệu suất về tốc độ tải trang và khả năng xảy ra lỗi.
* **Cần kĩ năng quản trị:**Mặc dù dễ sử dụng, nhưng để quản lý và duy trì một trang web WordPress lớn, cần có một số kiến thức về quản trị web, bao gồm việc quản lý cơ sở dữ liệu, bảo mật, và tối ưu hóa

# Lỗ hổng bảo mật và cách phòng chống

## Lỗ Hổng Brute Force

* **Định nghĩa**: là việc tấn công tiếp cận trang web bằng cách thử hàng nghìn tổ hợp tên tài khoản và mật khẩu cho đến khi tìm ra đúng thông tin đăng nhập.
* **Cách thức tấn công:**
* ***Xác định mục tiêu:*** sử dụng các bot lập trình để quét khắp internet và tìm kiếm các trang web chạy WordPress
* ***Tạo danh sách các tổ hợp***: Hacker sẽ tạo ra một danh sách các tổ hợp tên người dùng và mật khẩu. Danh sách này có thể được tạo ra một cách ngẫu nhiên hoặc dựa trên một từ điển chứa các mật khẩu phổ biến.
* ***Thử từng tổ hợp***: Các bot này tự động thử tất cả tổ hợp tên người dùng và mật khẩu phổ biến, thường được lấy từ kho dữ liệu
* ***Xác thực***: Các bot có khả năng thực hiện hàng nghìn lần đăng nhập mỗi phút và tiếp tục thử lại đến khi đoán đúng. Khi một tổ hợp đúng được tìm thấy, hacker sẽ có quyền truy cập vào hệ thống.
* **Nguyên nhân**:
* ***Giao diện đăng nhập mặc định***: Đường dẫn đăng nhập /wp-admin/ quá phổ biến, dễ dàng bị hacker phát hiện.
* ***Tên đăng nhập mặc định dễ đoán***:"admin" làm tên đăng nhập: Khi cài đặt WordPress lần đầu, nhiều người dùng để tên đăng nhập mặc định là "admin". Đây là một tên rất phổ biến và thường là mục tiêu đầu tiên của các cuộc tấn công brute force, giúp giảm nửa thời gian cần thiết cho việc tấn công.
* ***Mật khẩu yếu:*** Nhiều người dùng thường đặt mật khẩu quá đơn giản, dễ đoán.
* ***Thiếu các biện pháp bảo mật:*** Nếu không có các plugin bảo mật hoặc cấu hình bảo mật đúng cách, WordPress sẽ trở nên dễ bị tổn thương.
* **Hậu quả của tấn công Brute Force**
* Mất quyền kiểm soát website: Hacker có thể xóa dữ liệu, thay đổi nội dung, hoặc thậm chí sử dụng website của bạn để tấn công các website khác.
* Mất dữ liệu hoặc rò rỉ thông tin
* Lợi dụng website để phát tán malware: Website bị biến thành một nguồn phát tán mã độc tới những người truy cập khác.
* Thiệt hại về tài chính: Việc khắc phục hậu quả của một cuộc tấn công có thể tốn kém.
* **Cách phòng tránh:**
* ***Giới hạn số lần đăng nhập***: Đây là một giải pháp phổ biến và hiệu quả để ngăn chặn tấn công brute force. Ví dụ, bạn có thể cấu hình hệ thống chỉ cho phép người dùng nhập sai tên đăng nhập tối đa 3 lần, nếu không sẽ bị chặn IP truy cập hoặc tạm khóa tài khoản. Cài đặt plugin giới hạn đăng nhập như Limit Login Attempts Reloaded.
* ***Cài đặt xác thực hai yếu tố (2FA):*** Tăng cường bảo mật bằng cách yêu cầu một lớp xác thực thứ hai ngoài mật khẩu.
* ***Sử dụng mật khẩu mạnh:*** Khuyến khích người dùng tạo mật khẩu dài, phức tạp, và thay đổi mật khẩu định kỳ.
* ***Ẩn trang đăng nhập:*** Thay đổi URL trang đăng nhập hoặc sử dụng plugin để bảo vệ trang /wp-admin.

## SQL Injection

* **Định nghĩa:** là một kỹ thuật lợi dụng những lỗ hổng về câu truy vấn của các ứng dụng. Được thực hiện bằng cách chèn thêm một đoạn SQL để làm sai lệnh đi câu truy vấn ban đầu, từ đó có thể khai thác dữ liệu từ database**.**
* **Cách tấn công:**
* ***Xác định điểm yếu đầu vào:***Kẻ tấn công tìm kiếm các trang web có các trường đầu vào (như hộp tìm kiếm, form đăng nhập, form đăng ký) mà trong đó dữ liệu nhập vào không được kiểm tra hoặc lọc kỹ càng.
* ***Chèn mã SQL độc hại****:* kẻ tấn công sẽ nhập mã SQL độc hại vào các trường đầu vào.
* ***Khai thác cơ sở dữ liệu:*** sau khi xâm nhập thành công, tiến hành tấn công khác
* Ví dụ:
* Ở một trường nhập thông tin đăng nhập, thay vì nhập username và password thông thường, kẻ tấn công có thể nhập một chuỗi như: admin' OR '1'='1 để làm thay đổi ý nghĩa của truy vấn SQL.

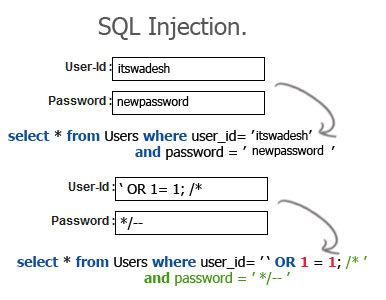
Truy vấn gốc để kiểm tra thông tin đăng nhập thường như sau:

SELECT \* FROM users WHERE username = 'admin' AND password = 'password';

Nếu kẻ tấn công nhập mã admin' OR '1'='1, truy vấn sẽ trở thành:

SELECT \* FROM users WHERE username = 'admin' OR '1'='1';

* Điều này sẽ khiến câu lệnh luôn trả về kết quả đúng vì điều kiện OR '1'='1' luôn đúng, cho phép kẻ tấn công vượt qua kiểm tra đăng nhập mà không cần mật khẩu hợp lệ.



* **Hậu quả:**
* Hack tài khoản cá nhân.
* Ăn cắp, thay đổi hoặc sao chép dữ liệu của trang web hoặc hệ thống.
* Chiếm quyền với tư cách quản trị viên.
* Xem thông tin cá nhân thuộc về những người dùng khác
* Sửa đổi cấu trúc của cơ sở dữ liệu, xóa các bảng thậm chí kiểm soát máy chủ cơ sở dữ liệu
* **Cách phòng tránh**:
* ***Cập nhật website thường xuyên và sử dụng tường lửa (Firewall***): Các bản cập nhật này thường vá các lỗ hổng bảo mật, bao gồm các vấn đề liên quan đến cơ sở dữ liệu, làm cho việc tấn công trang web trở nên khó khăn.
* ***Ẩn phiên bản WordPress***:Mỗi phiên bản WordPress có lỗ hổng riêng, việc công khai số phiên bản có thể tạo ra các mối đe dọa bảo mật và làm cho việc tấn công tiêm nhiễm SQL vào WordPress trở nên dễ dàng hơn cho tin tặc
* ***Xác thực dữ liệu người dùng***: đảm bảo rằng dữ liệu từ người dùng chỉ được chấp nhận nếu nó tuân theo định dạng cụ thể.Ví dụ, nếu trường địa chỉ email không có ký hiệu ‘@', thì dữ liệu không được chấp nhận.
* ***Giới hạn quyền truy cập và quyền của người dùng***: Điều này sẽ giảm quyền truy cập của người dùng vào cơ sở dữ liệu và ngăn chặn các cuộc tấn công SQL injection.
* ***Sử dụng Prepared Statements:*** Thay vì chèn trực tiếp dữ liệu vào câu lệnh SQL, nên sử dụng truy vấn tham số hóa (prepared statements) để tách biệt giữa mã SQL và dữ liệu đầu vào của người

## Phần mềm độc hại

* **Định nghĩa:** là loại mã độc được tiêm vào WordPress thông qua một chủ đề bị nhiễm, plugin lỗi thời hoặc tập lệnh. Mã này có thể trích xuất dữ liệu từ trang web của bạn cũng như chèn nội dung độc hại có thể không được chú ý do tính chất kín đáo của nó
* **Cách thức tấn công:**
* ***Phát hiện lỗ hổng***: sử dụng các công cụ quét tự động hoặc các kỹ thuật thủ công để tìm kiếm những lỗ hổng bảo mật trong WordPress, plugin, hoặc theme
* ***Tạo exploit***: Sau khi tìm ra lỗ hổng bảo mật, hacker sẽ viết một đoạn mã (exploit) để khai thác lỗ hổng dựa trên điểm yếu của plugin.theme
* ***Thực hiện tấn công***: Tải lên tệp độc hại hoặc chèn mã qua plugin/theme
* ***Xâm nhập hệ thống:*** 
  + Tạo cửa hậu (Backdoor) là tạo ra một cửa hậu để có thể quay lại hệ thống bất cứ lúc nào mà không cần phải thực hiện lại tấn công ban đầu
  + Chiếm quyền quản trị
  + Chèn mã độc vào trang web: để thực hiện các cuộc tấn công lừa đảo, phát tán mã độc, hoặc chuyển hướng người dùng đến các trang web lừa đảo khác.
* **Nguyên nhân:**
* Cài đặt plugin, theme không đáng tin cậy: Các plugin, theme từ nguồn không rõ ràng có thể chứa mã độc.
* Không cập nhật WordPress, plugin, theme: Các phiên bản cũ thường chứa nhiều lỗ hổng bảo mật.
* **Cách phòng tránh:**
* Chỉ nên tải xuống các chủ đề từ các tài nguyên đáng tin cậy
* Cập nhật thường xuyên: Cập nhật WordPress, plugin, và theme để vá các lỗ hổng bảo mật.
* Các plugin bảo mật như Succuri hoặc WordFence có thể được sử dụng để quét toàn bộ và sửa phần mềm độc hại.

## Cross-Site Scripting - XXS

* **Định nghĩa**: Lỗ Hổng Cross-Site Scripting (XSS):Kẻ tấn công có thể chèn mã JavaScript độc hại vào các phần của trang web (như biểu mẫu) để thực hiện hành vi tấn công như đánh cắp cookies hoặc thông tin người dùng.
* **Cách thức tấn công:**
* ***Chèn mã độc vào các trường nhập liệu***: Kẻ tấn công có thể nhập mã JavaScript vào các trường như ô tìm kiếm, form đăng nhập, hoặc bình luận.
* ***Sử dụng URL để gửi mã độc***: Mã độc có thể được chèn vào URL và khi người dùng truy cập vào URL đó, mã JavaScript độc hại sẽ được thực thi.
* ***Chèn mã vào các phản hồi của server:*** Nếu server không xử lý dữ liệu đầu vào đúng cách, mã JavaScript có thể được chèn vào phản hồi trả về và thực thi trong trình duyệt của người dùng.
* **Phân loại**
* ***Stored XSS***: Mã độc được lưu trữ trực tiếp vào cơ sở dữ liệu của website. Khi người dùng truy cập vào trang web, mã độc sẽ được hiển thị và thực thi.
* ***Reflected XSS:*** Mã độc được đưa vào trong các tham số của URL hoặc các yêu cầu HTTP khác. Khi người dùng click vào một liên kết độc hại, mã độc sẽ được thực thi.
* ***DOM-based XSS***: Mã độc được tiêm vào Document Object Model (DOM) của trang web. Điều này thường xảy ra khi các ứng dụng web sử dụng dữ liệu người dùng trực tiếp để tạo ra các phần tử HTML động mà không được kiểm tra, lọc kỹ lưỡng.
* **Nguyên nhân**
* ***Không kiểm tra và lọc dữ liệu đầu vào:***
  + Dữ liệu từ các trường form
  + Dữ liệu từ URL
  + Cookies và session
* ***Sử dụng các hàm output không an toàn:***
  + Không sử dụng các hàm escape: Việc không sử dụng các hàm escape để vô hiệu hóa các ký tự đặc biệt có thể dẫn đến việc mã độc được thực thi.
  + Không mã hóa các thuộc tính HTML: Nếu các thuộc tính HTML không được mã hóa đúng cách, kẻ tấn công có thể chèn mã JavaScript vào đó.
* **Cách phòng chống**
* ***Input validation (Xác thực đầu vào)****:* Mọi dữ liệu mà người dùng nhập vào đều phải được xác thực để đảm bảo rằng dữ liệu đó phù hợp với các quy tắc định sẵn. Chẳng hạn, nếu một trường chỉ chấp nhận số, thì bất kỳ ký tự nào khác số phải bị từ chối. Xác thực dữ liệu giúp giảm thiểu rủi ro mã độc hại từ các trường đầu vào, nhưng nó không hoàn toàn ngăn chặn XSS. Các biện pháp xác thực có thể bao gồm:
  + Hạn chế kiểu dữ liệu (như chỉ chấp nhận số hoặc chữ cái).
  + Đặt giới hạn độ dài của dữ liệu đầu vào.
  + Đảm bảo rằng các URL hay email được nhập vào đúng định dạng.
* ***Filtering (Lọc dữ liệu)****:* Các từ khóa nguy hiểm như <script>, javascript:, hoặc các thẻ HTML có thể bị loại bỏ, không cho phép các mã độc hại này lọt vào hệ thống. Tuy nhiên, các kẻ tấn công có thể tìm cách né tránh bộ lọc bằng cách thay đổi định dạng mã độc.
* Các bước thực hiện input filtering có thể bao gồm:
  + Xóa các thẻ <script>, <iframe>, hoặc các từ khóa như onload, onclick có thể kích hoạt mã JavaScript.
  + Loại bỏ các thuộc tính trong thẻ HTML liên quan đến sự kiện (event handlers) như onmouseover, onerror,...
* ***Escaping (Mã hóa dữ liệu đầu ra)****:* đảm bảo rằng dữ liệu đầu vào từ người dùng được mã hóa trước khi nó được xuất ra trình duyệt. Ví dụ, các ký tự đặc biệt như <, >, ", ' phải được chuyển thành các ký tự mã hóa tương đương (&lt;, &gt;, &quot;, &#39;). Điều này đảm bảo rằng bất kỳ đoạn mã độc nào được chèn vào cũng chỉ được hiển thị dưới dạng văn bản thông thường và không thể thực thi.
* Cách mã hóa này có thể được thực hiện cho:
  + Nội dung HTML.
  + Các thuộc tính HTML như giá trị của src, href,...
  + Các dữ liệu trong thẻ JavaScript hoặc CSS.

## Dịch vụ từ chối phân tán (DDoS)

* **Định nghĩa:** là một loại tấn công mạng nhằm làm quá tải một hệ thống bằng cách gửi khối lượng lớn yêu cầu đến một máy chủ web khiến nó chậm và cuối cùng gặp sự cố.
* **Cách thức tấn công:**
* ***Tạo botnet***: Kẻ tấn công sử dụng phần mềm độc hại để lây nhiễm hàng ngàn hoặc hàng triệu thiết bị trên toàn thế giới, biến chúng thành các bot (máy tính zombie) mà chúng có thể điều khiển từ xa.
* ***Làm quá tải hệ thống***: Khi kẻ tấn công quyết định mục tiêu, họ ra lệnh cho botnet thực hiện một lượng lớn yêu cầu (request) đến máy chủ hoặc hệ thống mạng của mục tiêu cùng một lúc. Số lượng yêu cầu quá lớn khiến máy chủ không thể xử lý kịp, dẫn đến quá tải và ngừng hoạt động.
* ***Gián đoạn dịch vụ:*** Kết quả của cuộc tấn công là trang web hoặc dịch vụ sẽ bị chậm đi đáng kể hoặc hoàn toàn không thể truy cập được do tài nguyên hệ thống (CPU, RAM, băng thông) bị tiêu hao hết để xử lý lượng yêu cầu khổng lồ.
* **Hậu quả của tấn công DDoS:**
* ***Ngừng hoạt động của dịch vụ***: Tấn công DDoS có thể khiến trang web, ứng dụng, hoặc dịch vụ mạng hoàn toàn ngừng hoạt động, làm gián đoạn trải nghiệm của người dùng.
* ***Thiệt hại tài chính:*** Doanh nghiệp sẽ mất doanh thu nếu trang web thương mại điện tử hoặc dịch vụ trực tuyến bị gián đoạn. Đồng thời, chi phí để khắc phục và bảo vệ trước các cuộc tấn công cũng tăng lên.
* ***Mất uy tín:*** Nếu một dịch vụ trực tuyến hoặc trang web thường xuyên bị gián đoạn do tấn công DDoS, khách hàng và người dùng sẽ mất niềm tin vào dịch vụ và có thể chuyển sang đối thủ cạnh tranh.
* ***Tăng chi phí lưu trữ:*** Một cuộc tấn công DDoS có thể sử dụng rất nhiều tài nguyên băng thông và lưu trữ, dẫn đến tăng chi phí dịch vụ lưu trữ cho chủ sở hữu trang web.
* **Cách phòng tránh:**
* ***Sử dụng dịch vụ CDN (Content Delivery Network):*** Các dịch vụ như Cloudflare hoặc Akamai có khả năng chống lại các cuộc tấn công DDoS bằng cách phân phối lưu lượng truy cập trên nhiều máy chủ toàn cầu.
* ***Tường lửa ứng dụng web (WAF):*** WAF có thể giúp lọc và ngăn chặn các yêu cầu độc hại trước khi chúng đến máy chủ, giảm thiểu nguy cơ làm quá tải hệ thống.
* ***Giám sát lưu lượng mạng***: Sử dụng các công cụ giám sát để phát hiện sớm các lưu lượng truy cập bất thường, từ đó có thể triển khai biện pháp ngăn chặn kịp thời.
* ***Tăng cường băng thông và tài nguyên hệ thống***: Mặc dù không phải là giải pháp toàn diện, nhưng việc tăng cường băng thông và tài nguyên máy chủ có thể giúp hệ thống chống chọi tốt hơn với các cuộc tấn công DDoS quy mô nhỏ.

## Cross-Site Request Forgery (CSRF)

* **Định nghĩa:** là một kiểu tấn công trong đó kẻ tấn công lừa người dùng thực hiện các hành động không mong muốn trên một ứng dụng web mà họ đã được xác thực.
* **Cách thức tấn công**
* ***Lợi dụng Phiên Làm Việc của Người Dùng***: Khi người dùng đăng nhập vào một trang web, ứng dụng sẽ lưu thông tin phiên (như cookie) để xác thực các yêu cầu tiếp theo. Kẻ tấn công khai thác thông tin phiên này để gửi yêu cầu giả mạo đến ứng dụng.
* ***Tạo Yêu Cầu Giả Mạo****:* Kẻ tấn công tạo ra một yêu cầu HTTP hợp lệ (như POST, GET) mà người dùng đã đăng nhập vào ứng dụng web gửi đến. Điều này có thể được thực hiện bằng cách chèn mã vào trang web độc hại mà người dùng sẽ truy cập.
* ***Lừa Người Dùng Thực Hiện Yêu Cầu***: Người dùng nhấp vào liên kết hoặc tải trang chứa mã độc. Mã này gửi yêu cầu đến ứng dụng web mà người dùng

đã đăng nhập, thực hiện các hành động như thay đổi thông tin cá nhân, gửi tin nhắn, hoặc thực hiện giao dịch tài chính.

* **Hậu quả**
* ***Tiết lộ thông tin cá nhân***: Kẻ tấn công có thể truy cập và đánh cắp thông tin cá nhân của người dùng, như tên đăng nhập, mật khẩu hoặc thông tin tài khoản ngân hàng.
* ***Mất dữ liệu quan trọng:*** xóa, chỉnh sửa hoặc thêm dữ liệu trên trang web mà người dùng đã đăng nhập.
* ***Mất niềm tin của khách hàng:*** Nếu một trang web bị tấn công CSRF và dẫn đến các vấn đề an ninh, khách hàng có thể mất niềm tin vào trang web và không muốn sử dụng nó nữa.
* ***Lây nhiễm malware:*** Nếu người dùng truy cập vào trang web đó, họ có thể bị lây nhiễm malware hoặc virus, gây hại cho máy tính hoặc thiết bị của họ.
* **Cách phòng chống**
* ***Đối với User:***người dùng nên tuân thủ một số nguyên tắc sau
  + Không nên lưu thông tin mật khẩu tại trình duyệt (không nên chọn các phương thức “lưu mật khẩu” hay “đăng nhập lần sau”
  + Nên đăng xuất thông tin đăng nhập vào tài khoản ngân hàng, tài khoản email, hay các trang mạng xã hội trên máy tính lạ
  + Không nên click vào đường link lạ
* ***Đối với Server***
  + **Sử dụng SameSite cookies:** SameSite cookies là một loại cookie được thiết kế để chỉ cho phép các yêu cầu từ cùng một trang web mà cookie đã được tạo ra, đảm bảo rằng các yêu cầu chỉ được gửi từ trang web gốc.
  + **Thiết lập Access-Control-Allow-Origin:** cho phép các trang web chỉ cho phép các yêu cầu từ các trang web cụ thể. Bằng cách giới hạn các trang web mà có thể gửi yêu cầu, các nhà phát triển có thể giảm thiểu nguy cơ tấn công CSRF.
  + **Sử dụng token CSRF:** Phương pháp này yêu cầu trang web tạo ra một token ngẫu nhiên và bao gồm nó trong các yêu cầu từ người dùng. Khi một yêu cầu được gửi đến trang web, token này được kiểm tra để đảm bảo rằng yêu cầu đó được gửi từ người dùng chính xác và không phải là một yêu cầu giả mạo.

# Demo

## Công cụ WPScan và Metasploit Framework

### WPScan

WPScan là một công cụ bảo mật mã nguồn mở dùng để quét và kiểm tra các lỗ hổng bảo mật trên các trang web chạy nền tảng WordPress. Nó được thiết kế chủ yếu cho các chuyên gia bảo mật và quản trị viên để tìm ra các lỗ hổng bảo mật phổ biến liên quan đến WordPress, như:

* Các plugin và theme dễ bị tấn công.
* Cấu hình bảo mật yếu.
* Người dùng WordPress với mật khẩu yếu hoặc dễ đoán.

Một số câu lệnh phổ biến của WPScan:

* Quét cơ bản một trang WordPress: wpscan --url <http://example.com>
* Quét plugin và theme có lỗ hổng: wpscan --url http://example.com --enumerate p,t
* Liệt kê người dùng WordPress:wpscan --url http://example.com –enumerate -u
* Tấn công brute force: wpscan --url http://example.com --passwords /path/to/passwords.txt --usernames admin

### Metasploit framework

Metasploit Framework là một framework viết bằng Ruby sử dụng để tấn công và khai thác những lỗ hổng trên nhiều loại hệ thống khác nhau.

Tính năng chính của Metasploit là khai thác lỗ hổng (Exploit): Metasploit chứa hàng nghìn module khai thác để tấn công các lỗ hổng bảo mật của các hệ thống và ứng dụng.

Một số khái niệm cơ bản:

* LHOST: Địa chỉ IP của máy Hacker (Nếu tấn công ngoài Internet thì xài IP Public, hoặc DDNS của No-IP.com)
* RHOST: Địa chỉ IP của máy Vicitm (Nếu tấn công ngoài Internet thì xài IP Public, RHOST có thể là URL Website cũng OK)
* LPORT: Port mở ra trên máy Hacker (Nếu tấn công ngoài Internet thì bắt buộc Port đó phải mở trên Router, còn hack trong mạng LAN thì port nào cũng được)
* RPORT: Port trên máy victim (Khi đi khai thác lỗ hổng, tùy lỗ hổng nằm trên giao thức nào thì có các RPORT đặc thù, thực chất Metasploit sẽ tự đặt cho các bạn)

Trong bài báo cáo này sẽ sử dụng hai công cụ trên để rà quét lỗ hổng và tấn công

## Tấn công Wordpress

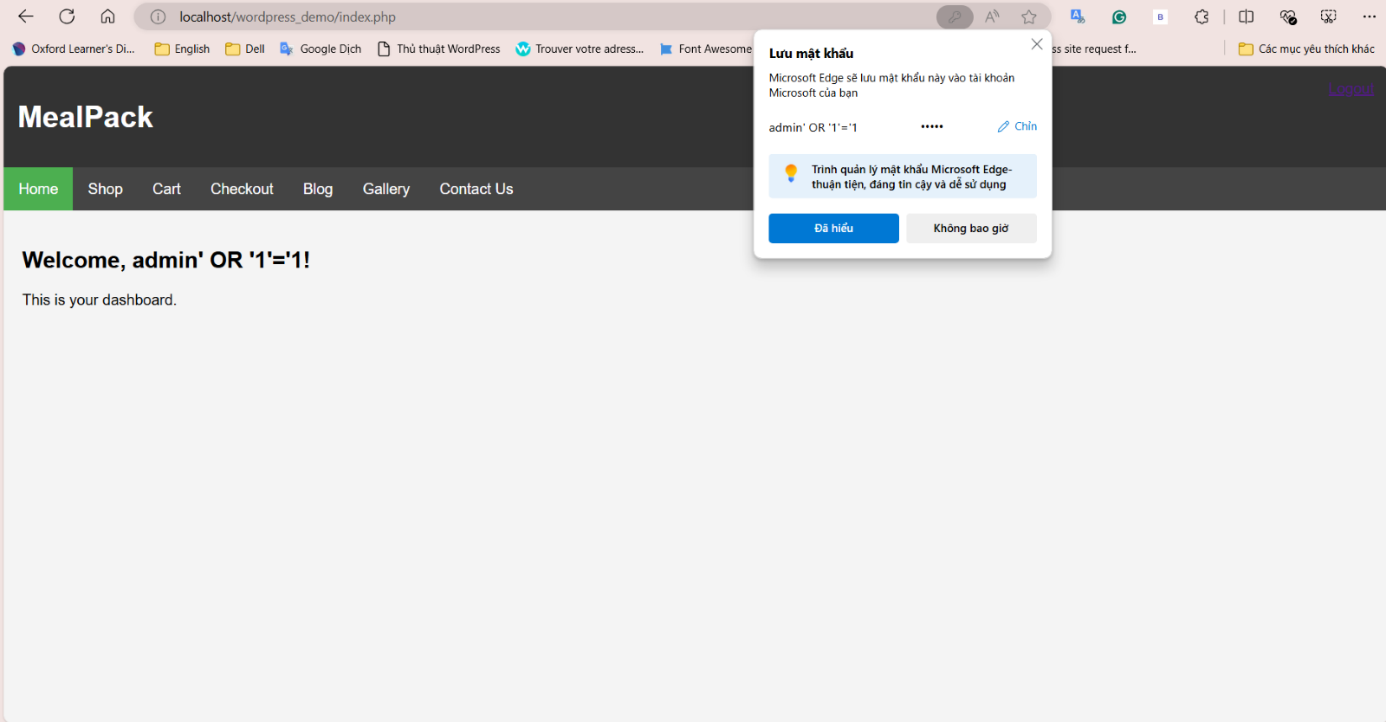
### Tấn công qua lỗ hổng SQL Injection

Tài khoản admin với mật khẩu: password123

A screenshot of a computer

Description automatically generated  
Điền ở ô tên đăng nhập: admin' OR '1'='1

* A screenshot of a computer

  Description automatically generated  
  Lúc này sẽ thông báo đăng nhập thành công do câu truy vấn đã bị thay đổi do chèn SQL
* 
* Câu truy vấn ban đầu bị đổi thành SELECT \* FROM users WHERE username = '' OR '1'='1' AND password = '';
* Do OR '1'='1' luôn đúng nên ta có thể bypass hệ thống xác thực và truy cập trái phép vào tài khoản

### Tấn công brute force

Tấn công trab có Url là http://blog.thm/

A screenshot of a computer

Description automatically generated

Dùng WPScan để quét tên người dùng:

A screenshot of a computer screen

Description automatically generated

Phát hiện người dùng kwheel, bjoel

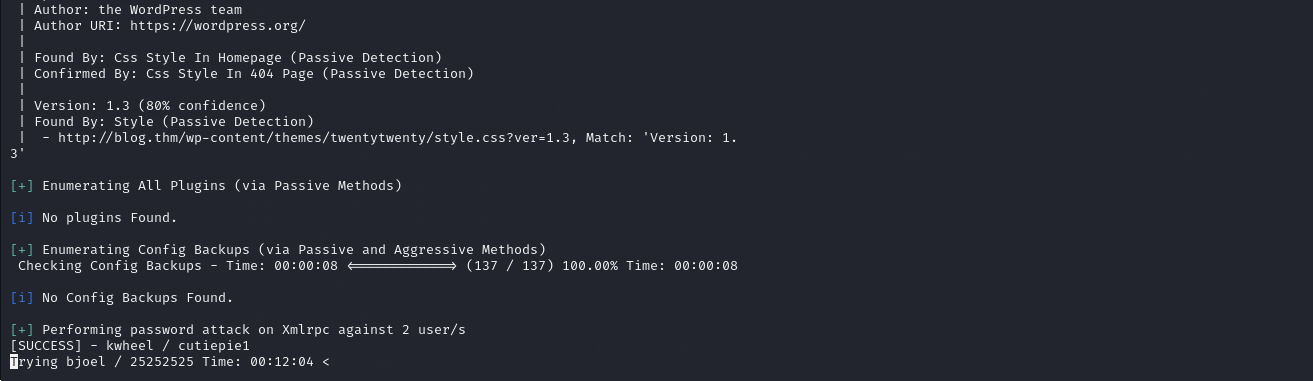
A screenshot of a computer

Description automatically generated

Quét mật khẩu dựa trên file rockyou.txt

A screenshot of a computer screen

Description automatically generated

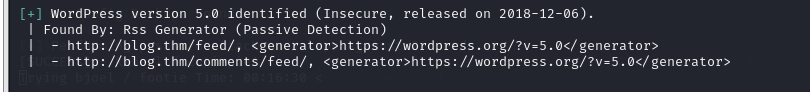


Tấn công thành công

A screenshot of a computer

Description automatically generated

### Tấn công qua lỗ hổng version Wordpress



Kiểm tra phiên bản Wordpress 5.0 ta thấy có lỗ hổng

Dùng metasploit để khai thác lỗ hổng

A screenshot of a computer program

Description automatically generated

Chuyển sang Shell để tương tác trực với hệ thống và kiểm tra file wp\_config.php

A screen shot of a computer

Description automatically generated

Truy cập và tìm được tài khoản mysql

A screenshot of a computer screen

Description automatically generated

Đăng nhập ta tìm thấy thông tin của user tuy nhiên mật khẩu đã được băm vậy nên ta tìm cách khác

A screenshot of a computer program

Description automatically generated

Tìm kiếm các file có quyền đặc biệt

A screenshot of a computer screen

Description automatically generated

Tìm thấy file lạ và tiến hành kiểm tra

A screenshot of a computer program

Description automatically generated

* Kiểm tra xem một chương trình đang làm gì bên trong bằng lệnh “ltrace”
* Ta thấy chương trình checker được thiết kế để kiểm tra xem biến môi trường "admin" có tồn tại hay không.Nếu biến này không tồn tại hoặc không có giá trị phù hợp, chương trình sẽ in ra thông báo "Not an Admin".
* Ta kiểm tra biến “admin” có tồn tại hay không.
* Do đó ta tạ biến admin và gán giá trị bằng 1
* Lúc này ra kiểm tra lại file checker và người dùng www-data đã cố gắng chuyển quyền thành root bằng cách sử dụng setuid(0)

Với quyền root ta truy cập vào cơ sở dữ liệu để đổi mật khẩu của admin

A screenshot of a computer program

Description automatically generated

Cuối cùng ta đã chiếm được quyền của admin:

A screenshot of a computer

Description automatically generated