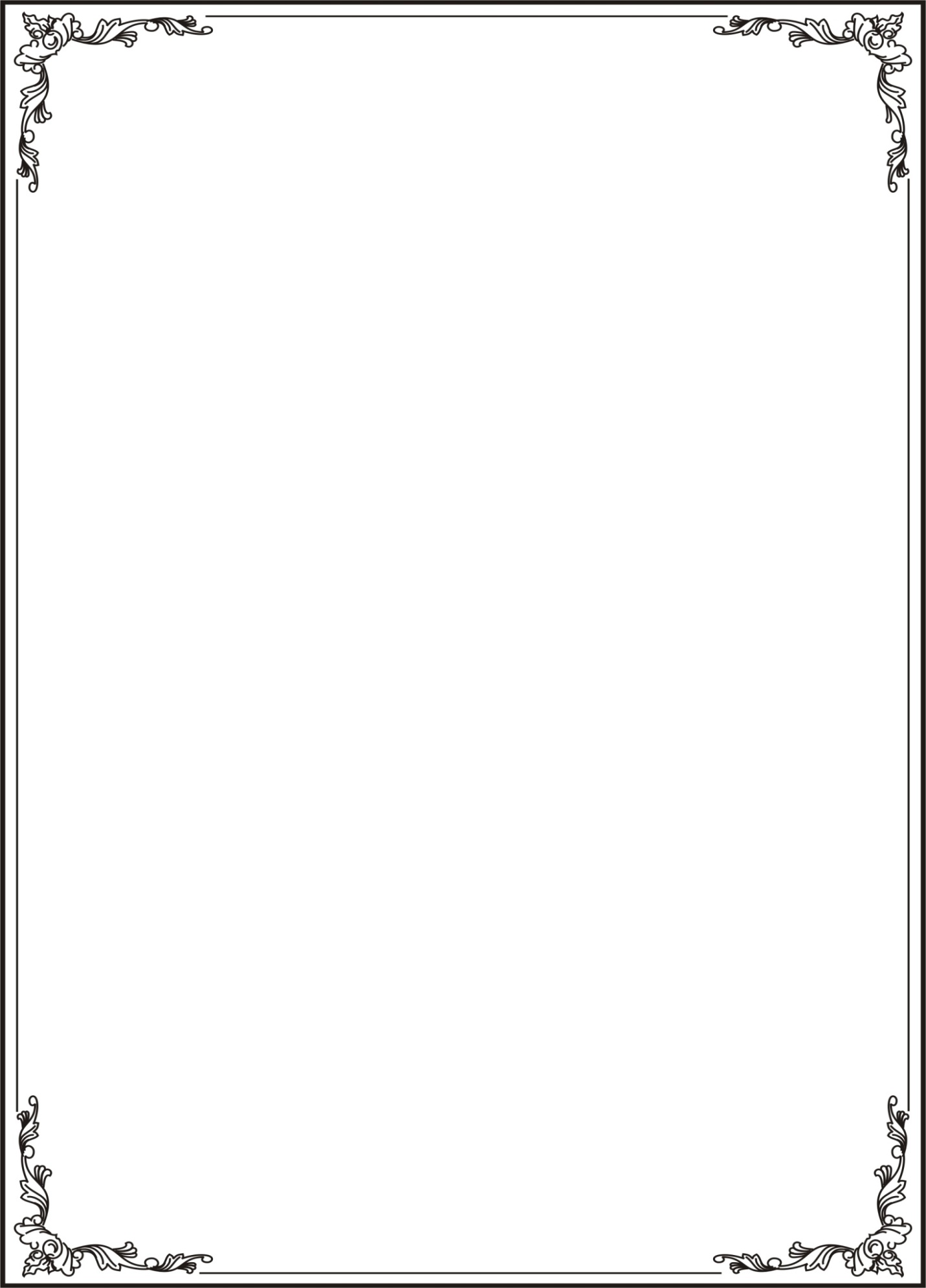
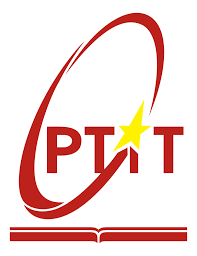
****

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔN**G

**KHOA CÔNG NGHỆ THÔNG TIN I**

-----🙞🙜🕮🙞🙜-----

****

**BÁO CÁO TIỂU LUẬN**

**MÔN AN TOÀN MẠNG NÂNG CAO**

**CHỦ ĐỀ: “TÌM HIỂU CÔNG CỤ WPSCAN”**

|  |  |  |
| --- | --- | --- |
| **Giảng viên hướng dẫn:** | TS. Đặng Minh Tuấn | |
| **Lớp:** | D17-111 | |
| **Sinh viên thực hiện:** | Bùi Đức Thắng | B17DCAT162 |

***Hà Nội, tháng 6/2021***

**MỤC LỤC**

[DANH MỤC TỪ VIẾT TẮT VÀ THUẬT NGỮ 3](#_Toc75984480)

[DANH MỤC HÌNH ẢNH 4](#_Toc75984481)

[LỜI NÓI ĐẦU 5](#_Toc75984482)

[CHƯƠNG 1: KHÁI QUÁT VỀ WORDPRESS 6](#_Toc75984483)

[1.1 WordPress là gì ? 6](#_Toc75984484)

[1.2 Các loại WordPress 7](#_Toc75984485)

[1.3 Các tính năng của WordPress 9](#_Toc75984486)

[CHƯƠNG 2: NHỮNG LỖ HỔNG THƯỜNG GẶP CỦA WORDPRESS WEB APPLICATION 10](#_Toc75984487)

[Sơ lược về lỗ hổng wordpress 10](#_Toc75984488)

[2.1 Lỗ hổng Backdoor 11](#_Toc75984489)

[2.2 Pharma Hacks 13](#_Toc75984490)

[2.3 Brute-force Login Attemps 13](#_Toc75984491)

[2.4 Malicious Redirect – Mã độc chuyển hướng 13](#_Toc75984492)

[2.5 Denial of Service – Tấn công từ chối dịch vụ 14](#_Toc75984493)

[CHƯƠNG 3: TỔNG QUAN VỀ WPSCAN TOOL 15](#_Toc75984494)

[3.1 Giới thiệu về WPScan 15](#_Toc75984495)

[3.1.1 WPScan là gì ? 15](#_Toc75984496)

[3.2.2 Các chức năng của WPScan 15](#_Toc75984497)

[Những điều WPScan có thể làm cho bạn là: 15](#_Toc75984498)

[CHƯƠNG 4: THỬ NGHIỆM CÁC CHỨC NĂNG 16](#_Toc75984499)

[4.1 Thông tin về thử nghiệm 16](#_Toc75984500)

[4.2 Các bước thử nghiệm 17](#_Toc75984501)

[4.2.1 Giải mã tệp tin bằng apktool 17](#_Toc75984502)

[4.2.2 Thực hiện phân tích mã nguồn 18](#_Toc75984503)

[4.2.3 Dựng lại tệp tin bằng apktool 20](#_Toc75984504)

[4.2.4 Tạo chữ ký 21](#_Toc75984505)

[4.2.5 Ký cho ứng dụng mới 22](#_Toc75984506)

[4.3 Kết quả thử nghiệm 23](#_Toc75984507)

[LỜI CẢM ƠN 24](#_Toc75984508)

[TÀI LIỆU THAM KHẢO 25](#_Toc75984509)

# DANH MỤC TỪ VIẾT TẮT VÀ THUẬT NGỮ

|  |  |
| --- | --- |
| **Từ viết tắt/thuật ngữ** | **Giải thích/giải nghĩa** |
| API | Application Program Interface |
| DDos | Distributed Denial of Service. Từ chối dịch vụ phân tán |
| DB | Database. Cơ sở dữ liệu |
| FTSP | Flooding Time Synchronization Protocol. Giao thức động bộ hóa thời gian ngập lụt |
| Plugin | Tiện ích tích hợp |
| SFTP | Secure File Transfer Protocol. Giao thức bảo mật truyền file |
| Theme | Chủ đề |
| WPScan | WordPress Scanning |
| URL | Uniform Resource Locator. Định vị tài nguyên thống nhất |

# DANH MỤC HÌNH ẢNH

[Hình 1: logo apktool 6](#_Toc74669452)

[Hình 2: phiên bản 2.5.0 7](#_Toc74669453)

[Hình 3: hai chức năng chính của apktool 8](#_Toc74669454)

[Hình 4: quy trình dựng ứng dụng bình thường 9](#_Toc74669455)

[Hình 5: mã bytecode smali 10](#_Toc74669456)

[Hình 6: quy trình giải mã của apktool 11](#_Toc74669457)

[Hình 7: quy trình dựng lại ứng dụng của apktool 12](#_Toc74669458)

[Hình 8: tải Java 13](#_Toc74669459)

[Hình 9: tiến hành cài đặt 13](#_Toc74669460)

[Hình 10: chọn thư mục cài JDK 14](#_Toc74669461)

[Hình 11: chọn thư mục cài JRE 14](#_Toc74669462)

[Hình 12: cài đặt hoàn tất 15](#_Toc74669463)

[Hình 13: mở properties 16](#_Toc74669464)

[Hình 14: mở Advanced system settings 17](#_Toc74669465)

[Hình 15: chọn Environment Variables 18](#_Toc74669466)

[Hình 16: thêm biến môi trường JAVA\_HOME 19](#_Toc74669467)

[Hình 17: tải apktool 20](#_Toc74669468)

[Hình 18: lab CTF 21](#_Toc74669469)

[Hình 19: demo giải mã bằng apktool 22](#_Toc74669470)

[Hình 20: hàm getFlag 22](#_Toc74669471)

[Hình 21: hàm nope 23](#_Toc74669472)

[Hình 22: hàm yep 23](#_Toc74669473)

[Hình 23: thay đổi mã nguồn hàm getFlag 24](#_Toc74669474)

[Hình 24: dựng lại bằng apktool 24](#_Toc74669475)

[Hình 25: tệp tin apk mới 24](#_Toc74669476)

[Hình 26: tạo chữ ký 25](#_Toc74669477)

[Hình 27: ký ứng dụng mới 26](#_Toc74669478)

[Hình 28: kết quả thử nghiệm 27](#_Toc74669479)

# LỜI NÓI ĐẦU

Ngày nay các web application ngày càng phổ biến trong cuộc sống hiện đại của con người. Chúng ta không thể phủ nhận những tiện lợi và các tài nguyên, thông tin mà các web application mang lại cho cuộc sống của con người. Mỗi ngày lại có hàng ngàn trang web khác nhau ra đời. Và khoảng 62% các web application trong số đó được làm bằng wordpress. Một báo các lỗ hổng ứng dụng web gần đây của Acunetix cho thấy khoảng 30% trong số các trang web WordPress hiện nay tồn lại các lỗ hổng tiềm tàng và dễ bị tấn công, khai thác. Điều đó khiến cho sự an toàn về dữ liệu, thông tin, tài nguyên của các nhà cung cấp nội dung cũng như của người dùng có thể bị đe dọa khi những lỗ hổng tiềm tàng trên các trang web Wordpress bị kẻ xấu lợi dụng và khai thác.

Wpscan là một công cụ miễn phí, vô cùng hữu ích trong trường hợp nếu bạn sở hữu một ứng dụng web Wordpress riêng và muốn đảm bảo sự an toàn và bảo mật cho trang web của bạn. Nó thực hiện một số công việc như: Kiểm tra xem trang web của bạn có sử dụng phiên bản Wordpress dễ bị tổn thương không, kiểm tra xem một theme hay plugin có được cập nhật hoặc dễ bị tấn công không, kiểm tra Timthumbs, kiểm tra sao lưu cấu hình, cơ sở dữ liệu,…

Trong báo cáo này, em sẽ trình bày khai quát về Wordpress, kết quả tìm hiểu về công cụ Wpscan và demo công cụ Wpscan trên một trang web thật để có thể có được kết quả trực quan nhất về công cụ này.

Trong quá trình tìm hiểu không thể tránh khỏi những thiếu sót. Mong thầy góp ý để em có thể hoàn thiện bài báo cáo một cách tốt nhất.

# CHƯƠNG 1: KHÁI QUÁT VỀ WORDPRESS

## 1.1 WordPress là gì ?

WordPress là phần mềm mã nguồn mở được cung cấp miễn phí, sử dụng ngôn ngữ lập trình PHP và hệ cơ sở dữ liệu MySQL. Do đó, nó thích hợp cho ai muốn đặt blog trên chính website sử dụng tên miền của riêng mình. Tuy nhiên, nếu không có tên miền riêng và chịu được một vài hình ảnh quảng cáo đôi khi xuất hiện, bạn vẫn có thể dùng chung với nhà cung cấp Automattic Production tại địa chỉ [http://wordpress.com](http://wordpress.com/) tương tự các nhà cung cấp khác.

WordPress là một dạng phần mềm mã nguồn mở, là hậu duệ chính thức của ***b2/cafelog***, được phát triển bởi Michel Valdrighi. Cái tên WordPress được đề xuất bởi Christine Selleck, một người bạn của nhà phát triển chính Matt Mullenweg.

WordPress viết bằng PHP và sử dụng hệ quản trị MySQL. WordPress chạy tốt trên PHP5, hầu hết mọi host (dịch vụ lưu trữ trực tuyến) có PHP đều hỗ trợ WordPress. Nhiều Host (Godaddy, Host Gator, …) còn có chức năng tự động cài đặt WordPress.

WordPress để đăng tải thông tin lên mạng, WordPress có chức năng như mọi Website khác. Nó có thể làm site tin tức, đánh giá, bán hàng… thậm chí là mạng xã hội.

Ngoài ra, WordPress còn hỗ trợ tạo Blog miễn phí trên WordPress.com để những ai không có điều kiện tài chính, kỹ thuật, thời gian… có thể sử dụng được WordPress.

WordPress còn thêm vào một số tính năng nhỏ nhằm hỗ trợ người dùng trong quá trình sử dụng như khả năng tự động lưu liên tục khi soạn thảo, nạp nội dung từ blog khác hay chia mục cho bài viết. Tuy nhiên, WordPress lại không có chức năng xem trước (preview) nội dung bài viết của mình, điều gây khó khăn cho người dùng khi họ cần xem xét và chỉnh sửa.

Các bản nâng cấp chính được chỉ định tên mã (*codenames*) đại diện cho các nhạc sĩ nhạc jazz nổi tiếng.



Hình 1: Logo WordPress

## 1.2 Các loại WordPress

*Wordpress* tạm được phân ra thành hai loại:

**Sử dụng dịch vụ của nhà cung cấp (*wordpress.com*).**

- WordPress.com là do 1 nhóm người dựa trên mã nguồn của WordPress tinh chỉnh lại để cung cấp dịch vụ tạo blog cho những người sử dụng, nhằm đơn giản hơn cho người dùng không chuyên. Khối lượng theme khá lớn, sử dụng mã nguồn mở PHP, tuỳ biến giao diện khá, xứng đáng là một đối thủ ngang tài đối với google blogger

- Giao diện thân thiện dễ sử dụng, cung cấp 50 kiểu giao diện khác nhau và cập nhật thường xuyên, hệ thống quản lý bài viết và comment mạnh mẽ, cho phép nhiều người cùng viết bài và cùng quản lý blog, kết nối với cộng đồng wordpress.com thông qua trang chủ, hỗ trợ tốt tiếng Việt và nhiều điểm nổi bật khác nữa.

**Trực tiếp cài trên host riêng (*wordpress.org*).**

*- Wordpress.org* là một thư viện khổng lồ của Wordpress. Nó gồm có mã nguồn Wordpress các phiên bản, các tài liệu hỗ trợ người dùng cũng như các nhà phát triển. Đồng thời, chứa số lượng khổng lồ các plugin và theme miễn phí (trong đó cũng không ít những theme có chất lượng). Và là nơi cung cấp mã nguồn của WordPress cho những blogger chuyên nghiệp hơn, nó đòi hỏi bạn phải có một domain và hosting riêng để viết blog.

- Wordpress.org không như wordpress.com, nó không phải là một dịch vụ để bạn có thể tạo blog trực tiếp lên đó. Bạn cần phải có domain, host hỗ trợ PHP/MySQL,.. để cài đặt mã nguồn này. Vì đây là hoàn toàn do bạn thực hiện nên bạn hoàn toàn làm chủ website của mình. Bạn có thể sử dụng được tất cả những tính năng hấp dẫn của Wordpress mà không cần phải trả thêm bất kỳ chi phí nào cho Wordpress.



Hình 2: Sự khác nhau giữa WordPress.com và WordPress.org

## 1.3 Các tính năng của WordPress

Khi tạo một blog cho riêng bạn có thể sẽ có những lý do riêng, nhưng nếu so với các script và dịch vụ blog khác, có thể bạn sẽ thích **Wordpress** ở những tính năng dưới đây.

* Dễ cài đặt, chỉ cần khởi tạo database, upload và thiết lập tham số trong file wp-config.php, sau 1,2 lần click chuột, bạn đã sẵn sàng để viết blog.
* Không giới hạn số lượng category và sub-category: bạn có thể tạo vô số chuyên mục và các chuyên mục con trong các chuyên mục chính mà không gặp phải bất kì rắc rối nào.Tự động xuất RSS và Atom: giúp cập nhật các thông tin về blog của bạn ngay lập tức.
* Sử dụng giao diện XML RPC để trackback và viết bài từ xa.
* Có thể đăng bài trên blog từ email.
* Hỗ trợ plugin và theme: đây là một điểm mạnh nhất của Wordpress. Nó tạo cơ hội cho hàng nghìn nhà phát triển cùng tham gia phát triển các plugin và theme cho Wordpress, làm cho nó càng ngày càng phong phú về tính năng và giao diện.
* Có thể nhập dữ liệu từ Blogger, Blogware, Bunny’s Technorati Tags, DotClear, GreyMatter, Jorome’s Keyword, LiveJournal, Movable Type, TypePad, RSS, Simple Tagging, Textpattern, B2evoluton, v.v. Đây là chức năng tuyệt vời nếu như bạn muốn chuyển từ một blog khác sang sử dụng Wordpress, nó giúp lại lấy lại tất cả các bài viết trên các blog khác để chuyển qua Wordpress.
* Rất nhiều tài liệu hướng dẫn để giúp phát triển thêm tính năng, và nhiều bộ API để mở rộng.
* Dễ quản lý và duy trì mà chẳng cần phải có nhiều kĩ năng hay kinh nghiệm
* Khả năng tìm kiếm trên blog rất tốt.
* Xuất bản nội dung ngay lập tức bất kể chiều dài của bài viết là bao nhiêu.
* Hỗ trợ viết blog đa ngôn ngữ.
* Administration Panel được tổ chức rất tốt với rất nhiều tính năng nhưng lại dễ hiểu và dễ sử dụng.
* Quản lý liên kết dễ dàng.

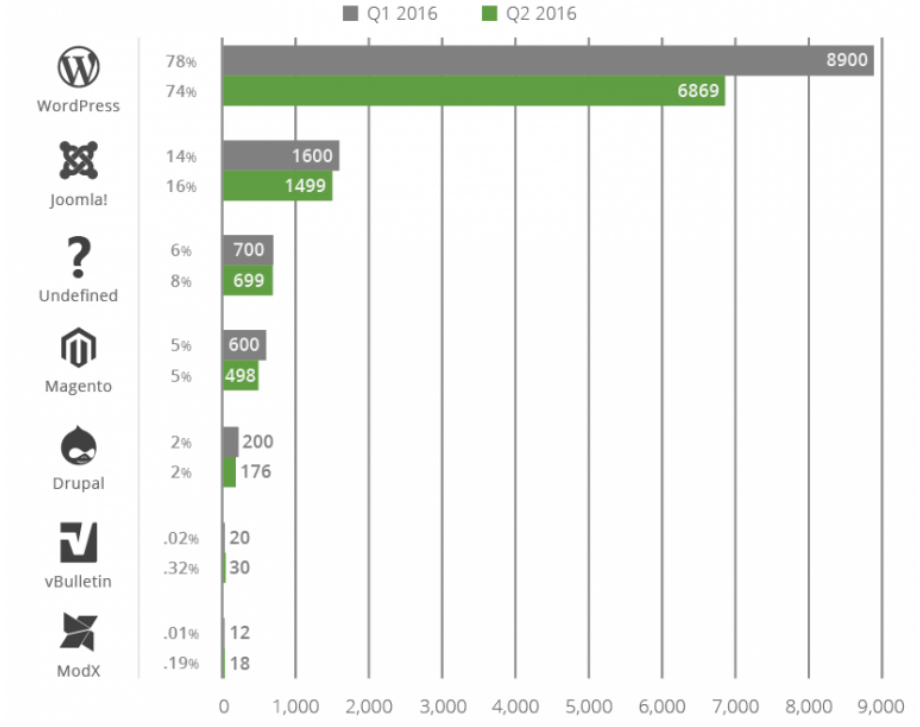
Với sự trợ giúp của các plugin và rất nhiều bộ API, bạn có thể chỉnh sửa Wordpress tùy thích theo nhu cầu của bạn, và thậm chí bạn cũng có thể sử dụng Wordpress để làm một website hoàn chỉnh. Wordpress có hàng ngàn plugin và theme, cộng với một đồng người sử dụng cực kì đông đảo luôn sẵn sàng góp sức phát triển, điều này làm cho Wordpress ngày càng lớn mạnh thể hiện vai trò số 1 của mình.

# CHƯƠNG 2: NHỮNG LỖ HỔNG THƯỜNG GẶP CỦA WORDPRESS WEB APPLICATION

## ****Sơ lược về lỗ hổng wordpress****

Wordpress đôi khi được đánh giá rằng kém bảo mật và không phải là một nền tảng an toàn dành cho doanh nghiệp. Hơn thế đây là một mã nguồn mở có cấu trúc khá cơ bản, thường xuyên tiềm ẩn các lỗ hổng bảo mật mà hacker có thể khai thác để tấn công vào website. Việc sử dụng một phiên bản wordpress đã cũ mà ko update, cộng với việc quản trị hệ thống yếu kém, thiếu kiến thức bảo mật cơ bản cần thiết sẽ làm cho website của bạn đối mặt với nhiều thách thức nguy hiểm. Ngay cả các hãng chuyên nghiệp như Reuterts cũng đã từng bị hack vào năm 2012 chỉ vì họ đang sử dụng một phiên bản wordpress quá cũ.

Nói vậy không phải lỗ hổng này không tồn tại trong giai đoạn hiện nay. Theo một nghiên cứu Q2  2016 thực hiện bởi Sucuri, một công ty bảo mật đa nền tảng. WordPress hiện vẫn tiếp tục dẫn đầu các trang web bị nhiễm mà họ đã thực hiện  chiếm 74%. Và ba plugins đầu tiên bị ảnh hưởng trên nền tảng này vẫn là Gravity Forms, TimThumb và RevSlider. Tuy nhiên điều này hiện có giảm xuống một chút từ Q1 năm 2016.



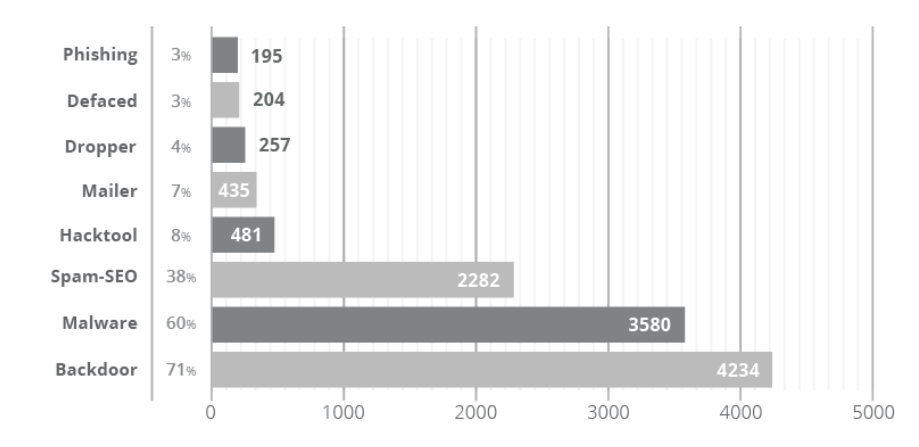
Hình 3: Báo cáo phân phối các nền tảng web bị lây nhiễm

## 2.1 Lỗ hổng Backdoor

Backdoor tên một lỗ hổng bảo mật được hacker khai thác với thuộc tính ẩn vượt qua các cơ chế mã hóa bảo mật để chiếm quyền truy cập vào các trang web WordPress không thông qua phương pháp truy nhập thông thường như wp-admin, SFTP, FTP, v..v..

Khai thác backdoor cho phép tin tặc có thể phá hoại dữ liệu trên máy chủ làm ảnh hưởng đến nhiều trang web được lưu trữ trên cùng một hosting. Đồng thời tạo đòn bẩy lây nhiễmchéo ra các website khác trên cùng máy chủ đó.

Tính trong quý 2 năm 2016 theo báo cáo của Sucuri, backdoors tiếp tục là một trong những cách thức được hacker sử dụng nhiều nhất, với 71% các trang web bị lây nhiễm đều bị dính backdoor.



Hình 4: Báo cáo phân phối các họ Malware

Backdoor thường được mã hóa để xuất hiện như các tập tin hợp pháp của hệ thống WordPress, và theo cách thực hiện của nó thông qua cơ sở dữ liệu WordPress để khai thác những điểm yếu, các lỗi trong phiên bản lỗi thời của nền tảng này. Những thất bại TimThumb là một ví dụ điển hình của backdoor khai thác lỗ hổng shady scripts và trên phiên bản wordpress quá cũ đã làm ảnh hưởng tới hàng triệu website.

Thật may mắn, vì phòng ngừa và xử lý lỗ hổng này khá đơn giản. Bạn có thể dùng công cụ SiteCheck để quét website của bạn, cái mà có thể dễ dàng phát hiện ra backdoor. Ngoài ra, xác thực 2 bước, chặn IP, hạn chế truy nhập admin và ngăn ngừa thực thi trái phép cá file php đơn giản từ các mối đe dọa của backdoor, cái mà chúng ta sẽ đi chi tiết hơn trong bài sau. Canton Becker có một bài viết tuyệt vời về cách làm sạch backdoor trên website wordpress của bạn.

## 2.2 Pharma Hacks

Pharma Hacks khái thác bằng cách chèn các code giả mạo vào các trang web wordpress của bạn hoặc các plugin phiên bản cũ, vì khi tìm kiếm trên các công cụ tìm kiếm nó sẽ trả về một quảng cáo cho các sản phẩm dược ở một trang web từ kết quả tìm kiếm mà đã được thỏa hiệp. Lỗ hổng này là thường nguy hiểm hơn các mối đe dọa spam mã độc truyền thống, khi website bị nhiễm thì các công cụ tìm kiếm sẽ chặn các website này và báo cáo website spam.

Chúng ta có thể làm sạch các Pharma Hack chưa các backdoor đến từ plugin và database, bạn có thể làm sạch theo hướng dẫn từ Sucuri Blog. Tuy nhiên, thường các biến thể  độc hại vẫn được mã hóa ẩn trong database và đòi hỏi một quá trình làm sạch triệt để sửa chữa các lỗ hổng. Hơn thế, cũng có thể khuyến nghị nhà cung cấp hosting thường xuyên update hệ thống máy chủ, update phiên bản cài đặt wordpress, các plugin kèm theo lên phiên bản mới.

## 2.3 Brute-force Login Attemps

Brute-force - Cố gắng login trang quản trị bằng cách thử nhiều mật khẩu là cách thức kẻ tấn công cố gắng đăng nhập bằng cách sử dụng script để khai thác mật khẩu yếu và có quyền truy nhập tới webstei của bạn. Xác thực 2 bước, giới hạn truy nhập, giám sát các truy nhập trái phép, block IP và dùng mật khẩu đủ mạnh là một vài cách thức dễ dàng và hiệu quả nhất để phòng chống tấn công Brute-force.  Theo thống kê, người dùng thường coi nhẹ vấn đề này, trung bình một ngày có nhiều hơn 30000 website bị tấn công bằng hình thức này.

## 2.4 Malicious Redirect – Mã độc chuyển hướng

Mã độc chuyển hướng tạo bởi backdoor trong bản cài đặt wordpress sử dụng FTSP; SFTP, wp-admin và các giao thức khác để chèn mã độc chuyển hướng website tới một trang khác. Chuyển hướng thường được đặt trong file .htacces và một file côt lõi khác trong website, nó thường là 1 scrpti được mã hóa  chuyển hướng website tới một trang web chứa mã độc.

Người dùng wordpress có thể sử dụng công cụ scan miễn phí để tìm các mã độ này giống như SiteCheck. Chúng tôi sẽ đi qua một số cách bạn có thể ngăn chặn những trong bước bảo mật WordPress của chúng tôi thêm dưới đây

## 2.5 Denial of Service – Tấn công từ chối dịch vụ

Có lẽ đây là mối đe dọa nguy hiểm nhất trong tất cả các  mối đe dọa hiện tại, ddos khai thác các lỗ hổng lỗi và sửa trong code để chiếm dụng hết bộ nhớ hệ thống. Hacker  thảo hiệp với hàng triệu website và chiếm hàng triệu dollar từ việc khai thác các phiên bản bản lỗi thời của wordpress  với các cuộc tấn công ddos. Mặc dù ít bị tấn công các trang web nhỏ tuy nhiên chúng bị lợi dụng để huy động tấn công các site doanh nghiệp lớn.

Ngay cả khi bạn đã sử dụng một phiên bản mới nhất của wordpress cũng chưa chắc bạn đã   tránh được các cuộc tấn công ddos, tuy nhiên bạn sẽ hạn chế được  hoặc tránh bị lợi dụng để  tham gia các cuộc tấn công bởi tổ chức tài chính và tội phạm mạng.

# CHƯƠNG 3: TỔNG QUAN VỀ WPSCAN TOOL

## 3.1 Giới thiệu về WPScan

### 3.1.1 WPScan là gì ?

WPScan là black box vulnerability scanner cho WordPress được viết bằng PHP chủ yếu tập trung vào các loại lỗ hổng khác nhau trong WordPress, WordPress themes, và plugins. Công cụ WPScan đã được cài đặt mặc định trong Kali Linux, SamuraiWTF, Pentoo, BlackArch và BackBox Linux. WPScan sử dụng cơ sở dữ liệu của tất cả các plugin và theme có sẵn (khoảng hơn 18000 plugins và 2600 themes) trong quá trình kiểm tra nhằm tìm ra các phiên bản lỗi thời và lỗ hổng bảo mật.



Hình 5: Logo WPScan

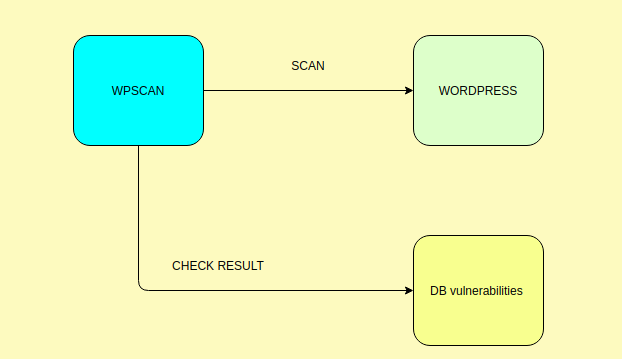
### 3.2.2 Các chức năng của WPScan

Những điều WPScan có thể làm cho bạn là:

* Phát hiện phiên bản WordPress hiện đang được cài đặt.
* Có thể phát hiện các tệp nhạy cảm như readme, robots.txt, cơ sở dữ liệu thay thế tệp,...
* Phát hiện các tính năng được kích hợt trên WordPress hiện đang được cài đặt.
* Liệt kê phiên bản và tên của theme.
* Phát hiện các plugin đã cài đặt và cho bạn biết nó đã lỗi thời chưa.
* Liệt kê tên các users.

**3.3.3 Luồng làm việc của WPScan**

* **Tool wpscan** : sẽ được sử dụng để check các version của wordpress như là phiên bản wordpress đang được sử dụng. Phiên bản của các plugin đang được sử dụng
* **Site wordpress** : Là một trang website được sử dụng wordpress
* **DB Vulnerabilities** : Là DB các lỗ hỏng được đã được phát hiện và được tập hợp lại. wpscan sẽ check lại xem có lỗ hỏng nào giống như trong DB không sẽ báo lại với người sử dụng wpscan. Được sử dụng API của DB lỗ hỏng wordpress.



* Bước 1 : Tool wpscan sẽ được gọi tới và kiểm tra các thông tin của wordpress như là phiên bản được cài đặt, các phiên bản của plugin được sử dụng ….
* Bước 2 : Sau đó kết quả sẽ được wpscan thu lại. Và nó sẽ sử dụng kết quả đó để check với DB Vulnerabilities
* Bước 3: Sau khi check xong với DB thì nếu như có lỗ hỏng nào được phát hiện nó sẽ trả về các lỗ hỏng đó hiển thị lên màn hình

# CHƯƠNG 4: HƯỚNG DẪN SỬ DỤNG WPSCAN

WPScan có thể được cài đặt trên rất nhiều các hệ điều hành khác nhau. Yêu cầu chung cho môi trường cài đặt của Wpscan là hỗ trợ ngôn ngữ Ruby bởi vì WPScan được viết bằng Ruby. Trong một môi trường dưới đây, cụ thể là hệ điều hành Ubutu, tôi sẽ hướng dẫn bạn sử dụng một vài chức năng cụ thể của công cụ WPScan.

## 4.1 Quét trang web cơ bản với WPScan

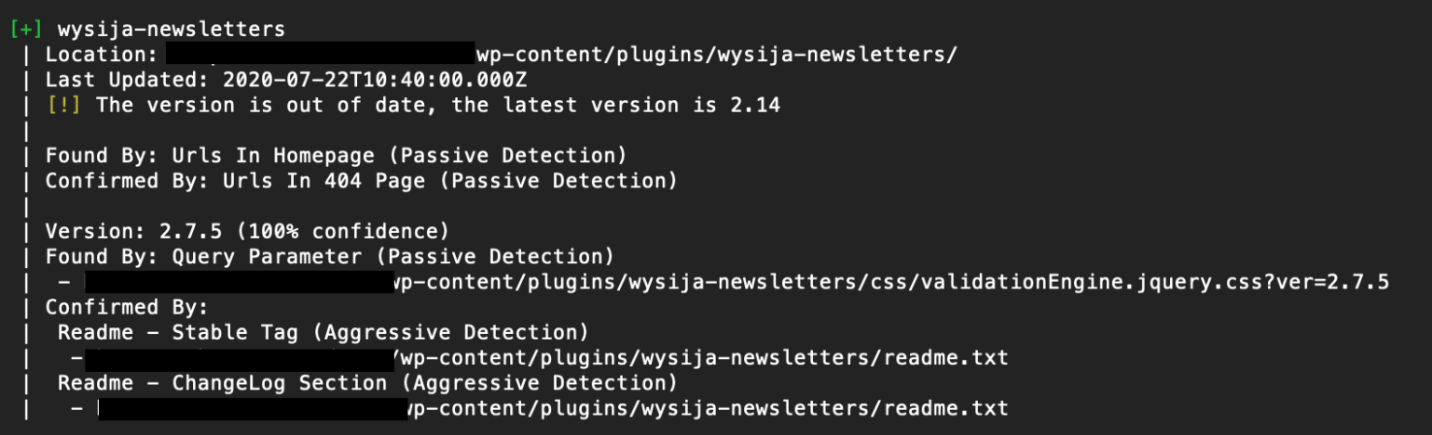
Khi sử dụng WPScan, lệnh của bạn sẽ luôn bắt đầu bằng wpscan và sau đó nó sẽ trỏ công cụ đến URL của bạn.

wpscan --url yourwebsite.com

Chạy lệnh trên sẽ thực hiện quét cơ bản trang web của bạn. Sau một vài phút, bạn sẽ có một loạt "Phát hiện thú vị" mà WPScan đã phát hiện ra từ mã trang web của bạn. Điều đó có thể bao gồm thông tin như:

* + Headers để khám phá thông tin máy chủ
  + Khả năng truy cập của xmlrpc.php
  + Khả năng truy cập của wp-cron.php
  + Phiên bản WordPress
  + Theme hoạt động và thông tin cơ bản của nó
  + Các plugin hoạt động và thông tin cơ bản của chúng
  + Sao lưu cấu hình có thể khám phá

Các cấu hình trang web và máy chủ khác nhau có thể tiết lộ thông tin khác nhau.



Các thông tin quét cơ bản khi chạy WPScan

Nếu web của bạn chạy bên dưới Firewall, thì bạn có thể thử quét với lệnh tương tự với một option thêm ở cuối câu lệnh

wpscan --url yourwebsite.com --random-user-agent

## 4.2 Xác định Theme & Plugin dễ bị tổn thương với WPScan

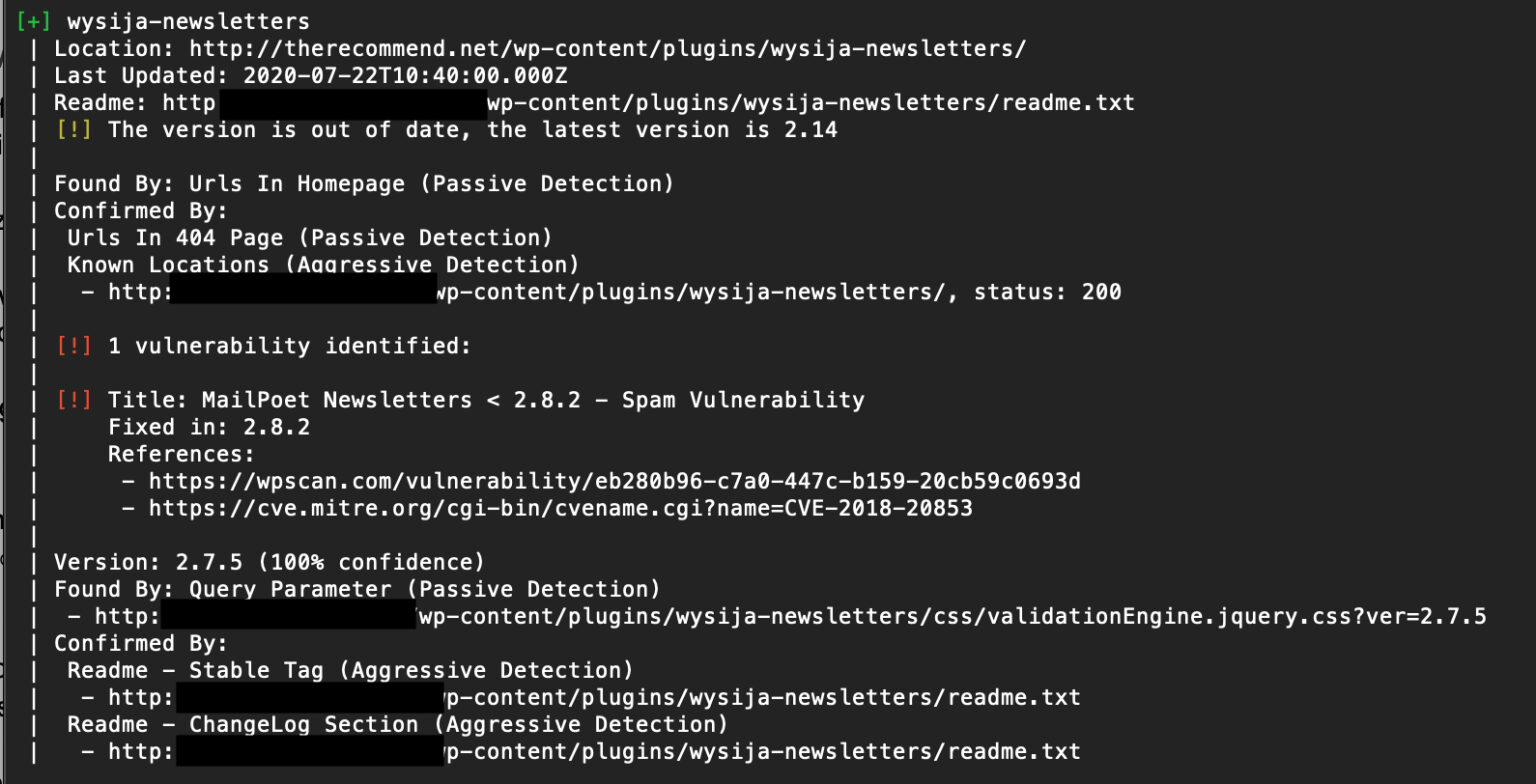
Mặc dù quá trình quét cơ bản sẽ cho bạn biết nếu một phiên bản chủ đề hoặc plugin đã lỗi thời, nó sẽ không cho bạn biết liệu có lỗ hổng cụ thể nào với phiên bản đó hay không. Để có được thông tin đó, bạn cần sử dụng API cơ sở dữ liệu lỗ hổng bảo mật WPScan.

Khi cài đặt WPScan, hãy đăng ký sử dụng API. Bây giờ, bạn sẽ chèn unique API token của mình vào bản quét để truy cập thông tin đặc biệt này. Bạn cũng sẽ thêm một số cờ bổ sung dựa trên thông tin cụ thể mà bạn muốn lấy. Điều quan trọng nhất trong trường hợp này là -e (viết tắt của "enumerate"-"liệt kê") và lựa chọn vp (“vulnerable plugins”-"plugin dễ bị tổn thương").

Dưới đây là lệnh phổ biến nhất để tìm kiếm các plugin dễ bị tấn công:

wpscan --url yourwebsite.com -e vp --api-token YOUR\_TOKEN

Hãy nhớ rằng quá trình này sẽ mất nhiều thời gian hơn so với quá trình quét cơ bản. Quá trình quét cơ bản kéo dài 5 phút của chúng tôi đã trở thành quá trình quét lỗ hổng trong 25 phút. Dưới đây là cùng một plugin được phát hiện từ quá trình quét ở trên, nhưng sử dụng cơ sở dữ liệu lỗ hổng bảo mật:

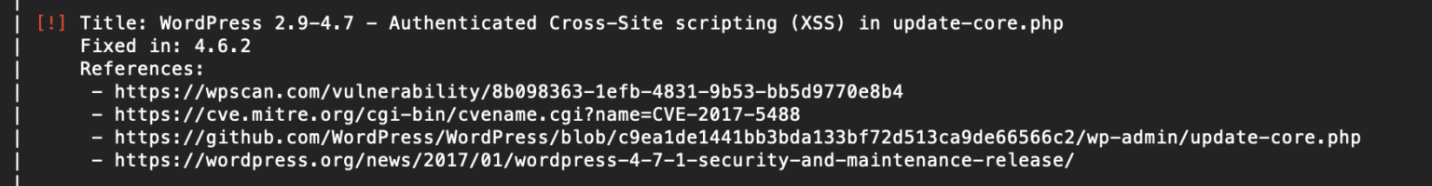


Thông tin plugin dễ bị tổn thương đã được quét với Wpscan

Để check Website của bạn có dùng Theme dễ bị tổn thương, thay option vp bằng vt (“vulnerable theme”):

wpscan --url yourwebsite.com -e vt --api-token YOUR\_TOKEN

Ngoài các lỗ hổng Theme hoặc plugin, WPScan cũng sẽ báo cáo bất kỳ lỗ hổng nào với phiên bản WordPress mà trang web của bạn đang chạy.

Các thông tin lỗ hổng với phiên bản WordPress

## 4.3 Kiểm tra danh sách người dùng bằng WPScan

Tuy nhiên, đừng dừng lại ở các plugin và chủ đề dễ bị tấn công. Các cuộc tấn công bằng mật khẩu gây ra một mối đe dọa lớn khác đối với bảo mật trang web của bạn. Và WordPress có thể cung cấp cho những kẻ tấn công quyền truy cập và thông tin quan trọng mà họ tìm kiếm. Với WPScan, bạn có thể xác định những tên người dùng nào có thể phát hiện được từ bên ngoài.

Để chạy quét bảng liệt kê này, chúng ta sẽ sử dụng lệnh sau:

wpscan --url yourwebsite.com -e u

WPScan sẽ sử dụng một số kỹ thuật khác nhau để tự đoán: xác định tên người dùng dựa trên thông tin có sẵn công khai trên trang web của bạn (tức là tên tác giả). WordPress sẽ thử nghiệm theo một số cách đặc biệt khi WPScan thăm dò những phỏng đoán đó. (Nội dung bôi đen bên dưới là ID người dùng được phát hiện.)



Danh sách người dùng được tìm thấy khi quét bằng WPScan

Chắc chắn là bạn không muốn bất kỳ tên người dùng nào có thể được khám phá bằng các kỹ thuật này. Cách dễ nhất để ngăn chặn điều đó là sử dụng các nick name hiển thị công khai khác với ID người dùng của bạn.

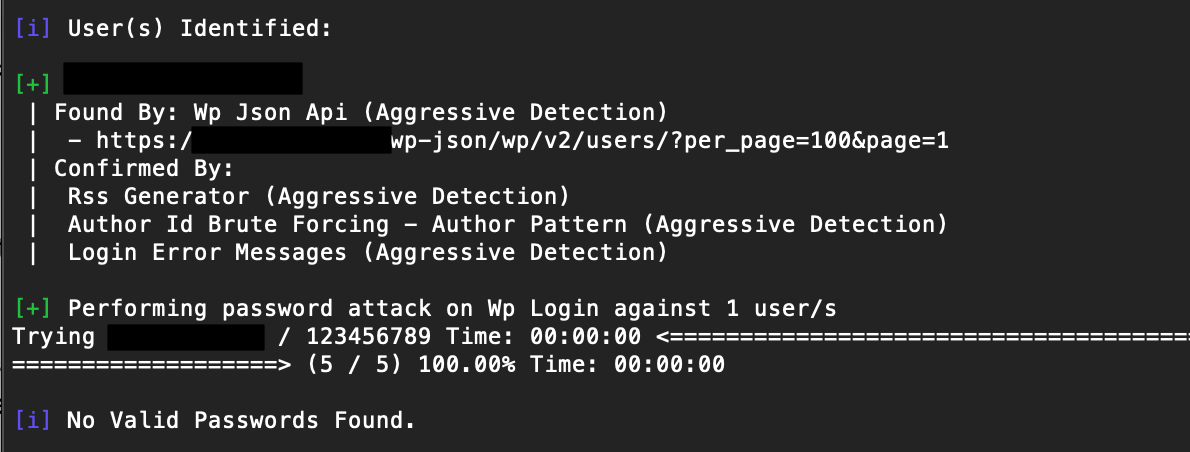
## 4.4 Kiểm thử tấn công mật khẩu với WPScan

Làm thế nào để kẻ tấn công theo dõi phát hiện ra tên người dùng? Tất nhiên, bằng cách cố gắng truy cập vào tài khoản của nó. WPScan thực sự cho phép bạn mô phỏng điều này. Và điều này sẽ đặc biệt hữu ích nếu trang web bạn đang quản lý có nhiều cộng tác viên: các trang web của công ty, blog cộng tác và những thứ tương tự.

Trước tiên, bạn cần lấy hoặc tạo danh sách mật khẩu. Với tìm kiếm nhanh trên Google, bạn có thể tìm thấy một số danh sách các mật khẩu được sử dụng phổ biến nhất, bao gồm cả danh sách từ rockou thường được sử dụng. Hãy nhớ rằng những danh sách này dài và bước này dẫn đến một cuộc tấn công vũ phu vào trang web được quét. Vì vậy, hãy lập kế hoạch phù hợp trước khi chạy quá trình quét này: ví dụ: Chuẩn bị máy chủ / quản trị viên của bạn, rút ngắn danh sách, sao chép trang web trong môi trường dàn dựng, chạy trong thời gian ngừng hoạt động của khách truy cập, v.v.

Để bắt đầu quét, lệnh sẽ là:

wpscan --url yourwebsite.com -passwords file/path/passwords.txt

  
Kết quả khi tiến hành quét attack password bằng WPScan

Trong quá trình quét ở trên, chúng ta đã chạy một danh sách ngắn gồm 5 mật khẩu phổ biến nhất dựa trên một trang web có một người dùng được liệt kê. Bởi vì người dùng đó không sử dụng bất kỳ mật khẩu nào trong số này, WPScan báo cáo “Không tìm thấy mật khẩu hợp lệ”.

# CHƯƠNG 5: DEMO SỬ DỤNG CÔNG CỤ WPSCAN

## 5.1 Môi trường thử nghiệm và demo

- Hệ điều hành: Kali Linux

- Mục tiêu quét và tấn công: Trang web WordPress thật

- Công cụ: WPScan, BurpSuite

- Ý tưởng: Sử dụng công cụ WPScan để rà quét một trang web sử dụng framework Wordpress để tìm các thông tin như phiên bản framework, phiên bản plugin, phiên bản theme đang sử dụng và các lỗ hổng tồn tại trong các thành phần đó,…

***Lời cam kết: Tất cả những thông tin quan trọng của trang web đều được tô đen để bảo mật thông tin. Những lỗ hổng bảo mật và thông tin bị khai thác đã được báo cáo lại cho nhà quản trị trang web để vá và sửa lỗi. Tất cả các thông tin khai thác được đều được sử dụng cho mục đích kiểm thử, không được sử dụng cho mục đích xấu.***

## 5.2 Thử nghiệm tấn công bằng WPScan với trang web thực tế

Bước 1: Lựa chọn trang web mục tiêu. Sau khi tìm kiếm các trang web sử dụng framework Wordpress thông qua google dork thì em đã chọn được một trang web sau để thử nghiệm rà quét bằng wpscan

A screenshot of a computer

Description automatically generated with medium confidence

Hình 1: Trang web mục tiêu

Bước 2: Sử dụng công cụ Burpsuite để lập sitemap cho trang web mục tiêu. Thông qua sitemap, có thể nhận thấy vị trí chứa thông tin về các plugin và theme mà trang web này sử dụng nằm tại /wp-content/plugins và /wp-content/themes

Graphical user interface

Description automatically generated with medium confidence

Hình 2: Sitemap của trang web

Bước 3: Sử dụng công cụ wpscan để thực hiện rà quét trang web bằng lệnh: **sudo wpscan --url target\_url -e ap,at,u --plugins-detection mixed --plugins-version-detection mixed --detection-mode mixed --wp-content-dir wp-content/ --wp-plugins-dir wp-content/plugins --api-token api\_key --random-user-agent**. Trong đó:

* **--url target\_url**: url trang web cần thực hiện rà quét
* **-e ap,at,u**: Các thông tin cần thu thập khi rà quét
  + **ap**: Tìm thông tin về tất cả các plugin mà trang web sử dụng
  + **at**: Tìm thông tin về tất cả các theme mà trang web sử dụng
  + **u**: Tìm thông tin về tất cả các user có trên trang web
* **--plugins-detection mixed**: Sử dụng chế độ mixed để thực hiện xác định các plugin mà trang web sử dụng. Chế độ này là kết hợp từ 2 chế độ là passive và aggressive
* **--plugins-version-detection mixed**: Sử dụng chế độ mixed để thực hiện xác định phiên bản của các plugin mà trang web sử dụng. Chế độ này là kết hợp từ 2 chế độ là passive và aggressive
* **--detection-mode mixed**: Sử dụng chế độ mixed để thực hiện xác định thông tin về theme mà trang web sử dụng và các user có trên trang web. Chế độ này là kết hợp từ 2 chế độ là passive và aggressive
* **--wp-content-dir wp-content/**: Cấu hình vị trí thư mục wp-content trên trang web. Dựa vào sitemap, có thể thấy thư mục wp-content nằm tại đường dẫn /wp-content
* **--wp-plugins-dir wp-content/plugins**: Cấu hình vị trí thư mục chứa thông tin về các plugin trên trang web. Dựa vào sitemap, có thể thấy thư mục wp-content nằm tại đường dẫn /wp-content/plugins
* **--api-token api\_key**: Cấu hình API key do WPscan cung cấp để tăng độ chính xác khi thực hiện rà quét
* **--random-user-agent**: Sử dụng một User-agent ngẫu nhiên nhằm tránh sự phát hiện của firewall

Graphical user interface, text

Description automatically generated

Hình 3: Wpscan bị firewall chặn khi không sử dụng --random-user-agent

Text

Description automatically generated

Hình 4: Thực hiện chạy wpscan để rà quét trang web

Bước 4: Phân tích kết quả thực hiện rà quét. Sau khi thực hiện rà quét bằng wpscan, kết quả thu được như sau:

Text

Description automatically generated

Hình 5: Kết quả thực hiện wpscan

Text

Description automatically generated

Hình 6: Kết quả thực hiện wpscan

Graphical user interface, text

Description automatically generated

Hình 7: Kết quả thực hiện wpscan

Graphical user interface, text

Description automatically generated with medium confidence

Hình 8: Kết quả thực hiện wpscan

Text

Description automatically generated

Hình 9: Kết quả thực hiện wpscan

Text

Description automatically generated

Hình 10: Kết quả thực hiện wpscan

Text

Description automatically generated

Hình 11: Kết quả thực hiện wpscan

Text

Description automatically generated

Hình 12: Kết quả thực hiện wpscan

Text

Description automatically generated

Hình 13: Kết quả thực hiện wpscan

Graphical user interface, text

Description automatically generated

Hình 14: Kết quả thực hiện wpscan

Dựa vào kết quả của wpscan, thu được các thông tin như sau:

* Trang web sử dụng ngôn ngữ PHP phiên bản 7.0.33 trên LiteSpeed Server
* Trang web có để file robots.txt có thể truy cập trực tiếp từ Internet

Text

Description automatically generated with medium confidence

Hình 15: File robots.txt

* Trang web có để file xmlrpc.php có thể truy cập trực tiếp từ Internet.. Thông qua file này, kẻ tấn công có thể thực hiện tấn công ddos hoặc brute-force mật khẩu user

Graphical user interface, text, application

Description automatically generated

Hình 16: File xmlrpc.php

* Trang web có để file wp-cron.php có thể truy cập trực tiếp từ Internet
* Trang web đang sử dụng phiên bản Wordpress 5.6. Phiên bản này có tồn tại các lỗ hổng như:
  + WordPress 5.6-5.7 - Authenticated XXE Within the Media Library Affecting PHP 8: Lỗ hổng XXE ảnh hưởng đến các phiên bản sử dụng PHP 8. Tuy nhiên, trang web đang sử dụng PHP phiên bản 7.0.33 nên không bị ảnh hưởng
  + WordPress 4.7-5.7 - Authenticated Password Protected Pages Exposure: Đây là lỗ hổng gây lộ nội dung các bài viết được bảo vệ bởi mật khẩu. Tuy nhiên lại yêu cầu có quyền truy cập vào 1 user nào đó trên trang web.
  + WordPress 3.7 to 5.7.1 - Object Injection in PHPMailer: Đây là lỗ hổng cho phép chèn một object trái phép. Tuy nhiên, lỗ hổng này chưa có exploit hay PoC được công bố
* Trang web đang sử dụng theme vtstheme và đang ở phiên bản mới nhất
* Hầu hết các plugin mà trang web đang sử dụng đều đang ở phiên bản mới nhất nên không tồn tại các lỗ hổng có thể khai thác
* Trang web để lộ các user có trên hệ thống thông qua đường dẫn /author-sitemap.xml

Graphical user interface, text, application

Description automatically generated

Hình 17: File author-sitemap.xml

* Trang web không tắt chế độ liệt kê các file trong thư mục

Graphical user interface

Description automatically generated with medium confidence

Hình 18: Chế độ liệt kê các file trong thư mục

Bước 6: Thực hiện khai thác các lỗ hổng có trên trang web:

* Thực hiện tấn công DDoS thông qua file xmlrpc.php:
  + Gửi request POST để xác định các method mà xmlrpc.php hỗ trợ

Graphical user interface, text, application

Description automatically generated

Hình 19: Method pinggback.ping

* + Nhận thấy trang web hỗ trợ method pingback.ping. Đây là 1 method cho phép trang web wordpress có thể gửi yêu cầu đến bất cứ máy chủ hoặc cổng nào
  + Kẻ tấn công có thể lợi dụng method này kết hợp cùng với method system.multicall để gửi cùng lúc nhiều request đến một máy chủ nào đó để thực hiện tấn công DDoS

Graphical user interface, application

Description automatically generated

Hình 20: Gửi request thông qua method pingback.ping

* Thực hiện tấn công brute-force mật khẩu user thông qua file xmlrpc.php
  + Gửi request POST để xác định các method mà xmlrpc.php hỗ trợ

Graphical user interface, application, Teams

Description automatically generated

Hình 21: Method wp.getUsersBlogs

* + Nhận thấy trang web hỗ trợ method wp.getUsersBlogs. Đây là 1 method cho phép lấy thông tin về các bài viết của 1 user trên trang web wordpress.
  + Kẻ tấn công có thể lợi dụng method này kết hợp cùng với method system.multicall và các user bị lộ thông qua /author-sitemap.xml để gửi cùng lúc nhiều request nhằm brute-force mật khẩu của 1 user nào đó

Graphical user interface, application

Description automatically generated

Hình 22: Thực hiện tấn công brute-force thông qua method wp.getUsersBlogs

LỜI CẢM ƠN

Trước tiên với lòng biết ơn sâu sắc nhất, chúng em xin gửi đến quý thầy cô tại Học viện Công nghệ Bưu chính Viễn thông lời cảm ơn chân thành vì đã cùng với tri thức và tâm huyết của mình để truyền đạt vốn kiến thức quý báu cho chúng em trong thời gian học tập tại học viện.

Trong học kỳ này, Học viện đã cho chúng em được học và tiếp cận với các môn học nền tảng rất hữu ích đối với sinh viên, đặc biệt là môn học “An toàn mạng nâng cao”. Bước đầu đi vào thực tế, tìm hiểu sâu hơn về môn học, kiến thức của chúng em còn hạn chế và các kỹ năng còn nhiều thiếu sót. Chúng em xin chân thành cảm ơn thầy Đặng Minh Tuấn đã tận tâm hướng dẫn chúng em thực hiện và hoàn thành môn học này của mình. Thầy đã luôn tạo điều kiện, nhiệt tình và đưa ra những lời khuyên, bài học bổ ích cho lớp chúng em trong suốt thời gian học môn học.

Cuối cùng chúng em xin kính chúc quý thầy cô đang công tác tại Học viện Công nghệ Bưu chính Viễn thông sức khỏe, niềm tin để tiếp tục thực hiện sứ mệnh cao đẹp của mình là truyền đạt kiến thức cho thế hệ nối tiếp.

Chúng em xin chân thành cảm ơn!

Hà Nội, tháng 6 năm 2021

Thắng

Bùi Đức Thắng

# TÀI LIỆU THAM KHẢO