

MỤC LỤC

Phần I. Những lời khuyên cần thiết cho bảo mật

1. Luôn luôn giữ phiên bản WordPress của bạn ở trạng thái cập nhật
2. Không tự ý thay đổi mã nguồn WordPress
3. Chắc chắn rằng tất cả plugin của bạn đã được cập nhật
4. Xóa tất cả các plugin và theme không kích hoạt hoặc không sử dụng
5. Đảm bảo tất cả các theme của bạn đã được cập nhật
6. Chỉ cài đặt theme, plugin và script từ các nguồn chính thống
7. Chọn một dịch vụ WordPress Hosting bảo mật tốt
8. Đảm bảo blog/ website của bạn đang chạy phiên bản PHP mới nhất
9. Thay đổi tên đăng nhập mặc định của quản trị viên
10. Luôn sử dụng mật khẩu đủ mạnh
11. Không tái sử dụng mật khẩu
12. Bảo vệ mật khẩu của bạn bằng cách tránh truyền tải mật khẩu bằng văn bản thuần túy
13. Chỉ cập nhật blog/ website của bạn từ các mạng internet đáng tin cậy
14. Sử dụng một phần mềm diệt virus trên máy tính
15. Kích hoạt Google Search Console
16. Bảo vệ WordPress bằng một plugin bảo mật
17. Thường xuyên sao lưu dữ liệu của blog/ website
18. Thường xuyên kiểm tra danh sách người dùng

Phần II. Các thủ thuật bảo mật WordPress căn bản

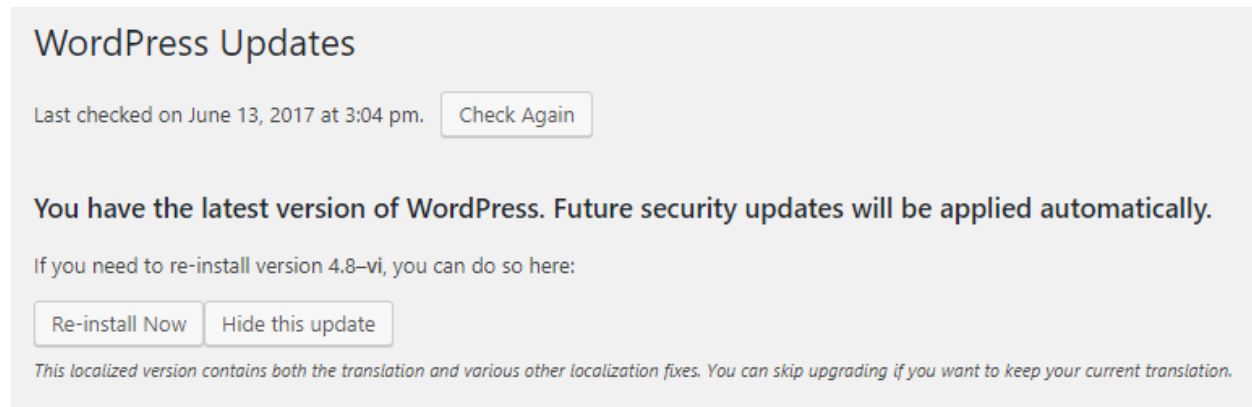
19. Cài đặt SSL cho blog/ website
20. Hạn chế số lần đăng nhập thất bại
21. Kích hoạt xác thực hai nhân tố (bảo mật 2 bước)
22. Bảo đảm chính xác quyền của tập tin và thư mục
23. Thay đổi tiền tố bảng mặc định của database
24. Đảm bảo bạn đã đặt khóa xác thực WordPress bí mật
25. Vô hiệu hóa thực thi tập tin PHP
26. Vô hiệu hóa “directory indexing và browsing”
27. Phân tách cơ sở dữ liệu WordPress của bạn
28. Hạn chế quyền của người dùng cơ sở dữ liệu
29. Vô hiệu hoá chỉnh sửa tập tin từ bảng quản trị WordPress
30. Bảo vệ tập tin wp-config.php của bạn
31. Bảo vệ tập tin .htaccess của bạn
32. Vô hiệu hoá XML-RPC (nếu bạn không sử dụng nó)
33. Vô hiệu hoá thông báo lỗi PHP
34. Cài đặt một tường lửa cho blog/ website
35. Sử dụng tường lửa của CDN
36. Theo dõi lịch sử đăng nhập và các thay đổi của tập tin

PHẦN I. NHỮNG LỜI KHUYÊN CẦN THIẾT CHO BẢO MẬT

1. Luôn luôn giữ phiên bản WordPress của bạn ở trạng thái cập nhật

WordPress được hỗ trợ bởi một cộng đồng vô cùng đông đảo. Nó thường xuyên nhận được các bản cập nhật. Đó có thể là bản cập nhật bổ sung tính năng mới, cải thiện hiệu năng, cũng có thể là một bản cập nhật giúp vá các lỗi bảo mật còn tồn tại trên các phiên bản cũ. Vì vậy, ngay khi có thông báo rằng một phiên bản WordPress mới đã được phát hành, bạn nên nhanh chóng nâng cấp blog/ website của mình.

Truy cập *Dashboard* => *Updates* và kiểm tra xem liệu bạn đang sử dụng phiên bản WordPress mới nhất hay chưa?



Nhiều bạn thường lo lắng khi cập nhật phiên bản WordPress mới, các plugin và theme chưa kịp thay đổi để tương thích, dẫn đến lỗi tính năng hoặc giao diện. Nhưng tôi chắc chắn rằng, bạn sẽ lựa chọn phương án thứ hai nếu phải đánh đổi giữa nguy cơ blog/ website bị hack và lỗi plugin/ theme. Bởi vì lỗi plugin/ theme thường chỉ tồn tại trong thời gian ngắn, các nhà phát hành sẽ nhanh chóng tung bản sửa lỗi để chúng tương thích với WordPress.

Và một lưu ý vô cùng quan trọng, trước khi cập nhật WordPress hay bất cứ plugin/ theme nào, các bạn nên tạo 1 bản sao lưu để đề phòng các sự cố có thể xảy ra.

Nếu bạn muốn update WordPress một cách hoàn toàn tự động, hãy thêm đoạn code sau đây vào file *wp-config.php*, bên trên dòng */* That's all, stop editing! Happy blogging. */*

```
define('WP_AUTO_UPDATE_CORE', true);
```

Trong trường hợp không thể cập nhật WordPress tự động, các bạn có thể cập nhật thủ công theo hướng dẫn trong bài viết [sau đây](#).

2. Không tự ý thay đổi mã nguồn WordPress

Để phục vụ cho một mục đích nào đó, nhiều bạn thường tự ý chỉnh sửa code trong các tập tin mã nguồn của WordPress (tất nhiên là ngoại trừ file *wp-config.php*). Điều này thực sự rất nguy hiểm. Nó không những có thể gây lỗi chức năng của WordPress mà còn là nguyên nhân dẫn đến việc blog/ website của bạn bị tấn công. Hacker có thể lợi dụng việc sửa đổi code của bạn (vô tình tạo

ra lỗ hổng) để bom mìn độc vào blog/ website. Do đó, tuyệt đối không nên tự ý chỉnh sửa mã nguồn của WordPress vì bất cứ mục đích gì.

3. Chắc chắn rằng tất cả plugin của bạn đã được cập nhật

Tương tự như mã nguồn WordPress (WordPress Core), bạn cũng cần phải giữ cho tất cả các plugin trên blog/ website của mình luôn ở trạng thái cập nhật.

Hãy truy cập *Dashboard* => *Updates* và kiểm tra xem tất cả chúng đã ở phiên bản mới nhất hay chưa? Nếu chưa, hãy cập nhật ngay lập tức.

Plugins

Your plugins are all up to date.

Điều này sẽ đảm bảo các plugins tương thích tốt nhất với phiên bản WordPress hiện tại, cải thiện hiệu suất, bổ sung thêm tính năng mới và thậm chí là vá các lỗ hổng bảo mật của chính nó. Rất nhiều blog/ website đã bị hack do sử dụng plugin ở phiên bản quá cũ. Đừng để bạn là nạn nhân tiếp theo.

Nếu bạn muốn update plugin một cách tự động, hãy thêm đoạn code sau đây vào file *wp-config.php*.

```
add_filter( 'auto_update_plugin', '__return_true' );
```

4. Xóa tất cả các plugin và theme không kích hoạt hoặc không sử dụng

Một số người dùng thường có thói quen cài rất nhiều plugin, theme. Và ngay cả khi không còn dùng đến nữa, họ vẫn không xóa chúng đi, thậm chí là không thêm deactivate. Điều này dẫn đến rất nhiều hệ lụy tiêu cực:

- Tiêu tốn dung lượng lưu trữ của host.
- Các plugin hoạt động gây tiêu tốn RAM, CPU, tăng page-size (nếu plugin đó có load thêm các file JS và CSS)... làm blog/ website của bạn trở nên ì ạch.
- Những plugin này có thể là công cụ tiếp tay cho hacker xâm nhập vào blog/ website của bạn, thông qua các lỗi bảo mật của chúng.

Vậy nên, nếu không có nhu cầu sử dụng plugin/ theme nào đó, các bạn nên deactivate và xóa tất cả chúng đi cho đỡ... rắc rối.

5. Đảm bảo tất cả các theme của bạn đã được cập nhật

Vấn đề này hoàn toàn tương tự với việc update WordPress Core và plugin nên tôi sẽ không nói thêm nữa. Để kiểm tra các phiên bản cập nhật cho theme, các bạn chỉ cần truy cập *Dashboard* => *Updates* là được.

Themes

Your themes are all up to date.

Còn nếu muốn thiết lập để update theme một cách tự động (thường chỉ áp dụng được với các theme miễn phí được cài đặt từ WordPress.org), hãy thêm code sau đây vào file *wp-config.php*.

```
add_filter( 'auto_update_theme', '__return_true' );
```

6. Chỉ cài đặt theme, plugin và script từ các nguồn chính thống

Đây là vấn đề mà không ít bạn mắc phải. Do điều kiện kinh tế hạn hẹp nhưng lại muốn sử dụng theme/ plugin cao cấp (trả phí) nên một số người dùng đã “làm liều”, download theme/ plugin trả phí từ các trang chia sẻ lậu (nulled). Nhưng các bạn nên nhớ một điều rằng: không có cái gì trên đời này là hoàn toàn miễn phí. Những theme/ plugin được chia sẻ tràn lan kia tiềm ẩn rất nhiều nguy cơ về bảo mật. Chúng có thể chứa malware, backdoor, shell, backlinks ẩn... cùng vô vàn những thứ độc hại khác. Và hậu quả thì chắc bạn đã biết rõ:

- Bị hacker chiếm quyền kiểm soát site.
- Bị đánh cắp hoặc xóa dữ liệu trên blog/ website.
- Bị các trình duyệt web cảnh báo nguy hiểm
- Bị các công cụ tìm kiếm đánh tụt hạng, thậm chí là xóa hoàn toàn khỏi kết quả tìm kiếm của họ.

Vậy nên, lời khuyên chân thành là đừng bao giờ nghĩ đến việc sử dụng theme/ plugin “lậu” nếu bạn muốn xây dựng blog/ website một cách nghiêm túc. Chỉ download theme và plugin từ các nguồn chính thống.

Nếu có điều kiện kinh tế quá eo hẹp, bạn có thể xem xét tham gia chương trình “mua chung” theme và plugin của *WP Căn bản* [tại đây](#). Các sản phẩm của chúng tôi đều có nguồn gốc rõ ràng, cam kết chính hãng và hỗ trợ update thường xuyên.

7. Chọn một dịch vụ WordPress Hosting bảo mật tốt

Hosting là một trong những yếu tố quan trọng, quyết định mức độ an toàn cho blog/ website của bạn. Kể cả khi bạn bảo mật mã nguồn WordPress cực tốt, nhưng hosting lại tồn tại nhiều lỗ hổng thì nguy cơ blog/ website của bạn bị tấn công vẫn còn đó.

Thông qua hosting, hacker có thể thực hiện các phương thức tấn công như local attack, even 0-day hacks... và dễ dàng chiếm quyền điều khiển hay bom mã độc vào blog/ website của bạn.

Vậy nên, khi mua hosting, các bạn nên lựa chọn các nhà cung cấp lớn, uy tín, có trang bị hệ thống quét mã độc, cảnh báo virus, tường lửa... chẳng hạn như *HawkHost*, *StableHost*, *SiteGround*...

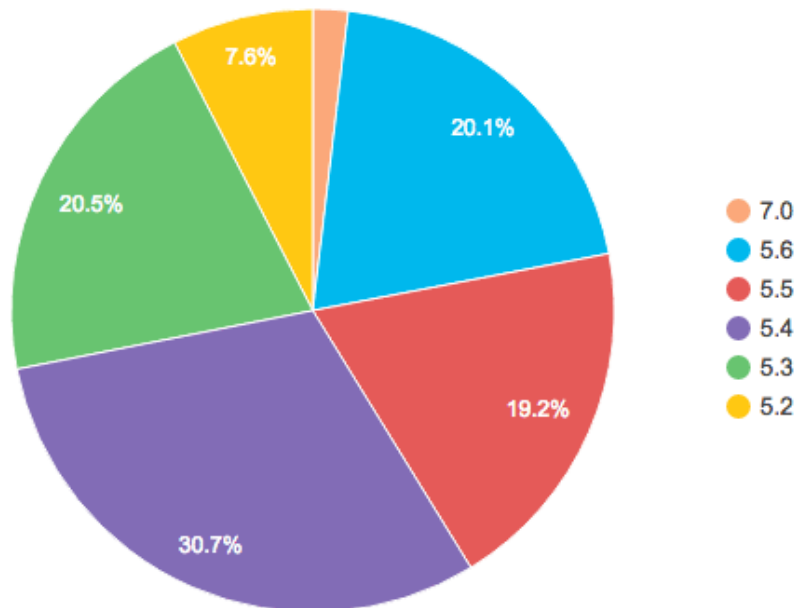
Qua một thời gian dài nghiên cứu và tìm hiểu, chúng tôi đã tổng hợp được danh sách một số nhà cung cấp WordPress Hosting giá rẻ, chất lượng tốt, các bạn có thể tham khảo [tại đây](#).

Ngoài ra, *WP Căn bản* cũng đang kết hợp với *HawkHost* để cung cấp dịch vụ WordPress Hosting giá rẻ, chất lượng cao, bảo mật tốt. Nếu các bạn có nhu cầu có thể tìm hiểu thêm [tại đây](#).

8. Đảm bảo blog/ website của bạn đang chạy phiên bản PHP mới nhất

Một báo cáo của WordPress.org đã cho thấy: hiện chỉ có 1.7% số blog/ website WordPress đang chạy trên phiên bản PHP 7.0 và 19.8% chạy trên PHP 5.6. Đây là 2 phiên bản PHP vẫn đang tiếp tục được hỗ trợ và cập nhật.

PHP Versions



Điều đó có nghĩa là gần 80% số site còn lại đang chạy trên các phiên bản PHP không còn được hỗ trợ nữa. Một phiên bản PHP không còn được hỗ trợ sẽ không được bổ sung các bản vá lỗi bảo mật. Và hậu quả thì không cần nói chắc các bạn cũng đã rõ.

Vì vậy, trước khi có ý định đặt mua hosting, các bạn nên tìm hiểu xem nhà cung cấp đó có hỗ trợ phiên bản PHP mới nhất cho hosting của họ hay không? Nếu có, hãy chuyển sang sử dụng phiên bản PHP mới cho blog/ website của bạn ngay khi có thể.

WP Căn bản đã từng có một bài hướng dẫn thiết lập PHP 7.x tối ưu cho mã nguồn WordPress, các bạn có thể tham khảo thêm [tại đây](#).

9. Thay đổi tên đăng nhập mặc định của quản trị viên

“admin” hay “administrator” là những cái tên đăng nhập thường được sử dụng nhiều nhất trong quá trình cài đặt WordPress. Một số bạn vì quá lười nghĩ tên đăng nhập mới hoặc muốn dùng

một cái tên thông dụng cho dễ nhớ mà vô tình đặt blog/ website của mình vào trạng thái nguy hiểm.

Để thực hiện một cuộc tấn công brute force nhằm chiếm quyền điều khiển blog/ website, các hacker thường phải trải qua 2 bước: tìm tên đăng nhập và tìm mật khẩu đăng nhập. Sử dụng tên đăng nhập mặc định như “admin”, “administrator” đồng nghĩa với việc bạn đã giúp chúng vớt bở được một nửa gánh nặng. Công việc còn lại chỉ còn là tìm ra mật khẩu chính xác nữa mà thôi.

Vậy nên, nếu bạn đang sử dụng tên đăng nhập mặc định hoặc quá dễ để tìm ra, hãy nhanh chóng đổi sang tên mới để đảm bảo an toàn cho blog/ website.

Cách thức đổi tên đăng nhập cũng khá đơn giản, các bạn chỉ cần làm theo một trong 2 hướng dẫn sau đây:

- [Làm thế nào để thay đổi tài khoản Admin trong WordPress](#)
- [Hướng dẫn thay đổi Username trong WordPress](#)

10. Luôn sử dụng mật khẩu đủ mạnh

Để dễ nhớ, nhiều bạn thường đặt mật khẩu đăng nhập rất đơn giản, chẳng hạn như: 123456789, password, matkhu, admin...

Nhưng các bạn không biết rằng đây chính là nguyên nhân khiến blog/ website của mình dễ bị hack theo phương thức brute force attack. Những mật khẩu dạng như trên quá thông dụng và quá dễ bị đoán ra. Chúng thường được hacker thử đầu tiên và không mất quá nhiều thời gian tìm kiếm.

Nếu muốn đảm bảo an toàn cho blog/ website, mật khẩu đăng nhập tài khoản quản trị của bạn nên tuân thủ các quy định sau đây.

- Có ít nhất 8 ký tự. Tất nhiên càng dài thì càng tốt.
- Không nên là một từ hoặc cụm từ có ý nghĩa.
- Không nên là ngày sinh hay tên của bạn.
- Có chứa ký tự in hoa, in thường, chữ số và các ký tự đặc biệt (như ~!@#).

Nếu mật khẩu mà bạn đang sử dụng chưa thỏa mãn các điều kiện trên, ngay bây giờ, hãy truy cập vào *Users => Your Profile => New Password* và tạo cho mình mật khẩu mới đủ mạnh.

The screenshot shows the 'Account Management' section of a WordPress dashboard. Under the 'New Password' heading, there is a text input field containing the password 'DdbpbuSuZfQsx9^sPVIS&eMw'. Below the input field, a green bar indicates the password strength as 'Strong'. To the right of the input field are two buttons: 'Hide' (with an eye icon) and 'Cancel'.

Để dễ dàng hơn, các bạn có thể nhờ sự trợ giúp của công cụ [Secure Password Generator](#).

11. Không tái sử dụng mật khẩu

Nếu bạn nghĩ chỉ cần tạo một mật khẩu đủ mạnh và sau đó sử dụng nó trên nhiều tài khoản khác nhau thì đó thực sự là một sai lầm nghiêm trọng. Hacker nắm được nhược điểm đó của người dùng. Và chỉ cần họ xâm nhập được một tài khoản, những tài khoản khác cũng sẽ nằm trong diện bị tấn công.

Do đó, lời khuyên chân thành là bạn nên sử dụng mật khẩu khác nhau cho mỗi tài khoản. Đây không phải là thủ thuật bảo mật dành riêng cho WordPress mà là thủ thuật bảo mật thông tin nói chung.

Nếu việc sử dụng quá nhiều mật khẩu khác nhau khiến bạn không thể nhớ hết được, hãy sử dụng các công cụ chuyên dụng như [Intel True Key](#) hay [RoboForm](#) để lưu thông tin đăng nhập. Không nên lưu thông tin đăng nhập trên trình duyệt web vì chúng rất dễ bị xóa mất hoặc bị đánh cắp.

12. Bảo vệ mật khẩu của bạn bằng cách tránh truyền tải mật khẩu bằng văn bản thuần túy

Dữ liệu nhạy cảm như thẻ tín dụng và mật khẩu không bao giờ nên được gửi ở dạng không được mã hóa. Bởi vì trên thực tế có rất nhiều công cụ và máy phân tích có khả năng đánh cắp dữ liệu của bạn.

Hãy chắc chắn bạn đã bảo vệ tốt mật khẩu của mình bằng cách sử dụng các kỹ thuật phòng ngừa sau đây:

- Không gửi mật khẩu qua email, chat, mạng xã hội hoặc các dạng truyền tin khác nếu chúng không được mã hóa.
- Cài đặt SSL và sử dụng giao thức HTTPS trên blog/ website WordPress của bạn, đặc biệt là trên trang đăng nhập và trang quản trị, để tránh các mật khẩu được gửi bằng văn bản thuần túy. Bạn có thể tìm hiểu việc cài SSL cho blog/ website WordPress thông qua bài viết [sau đây](#).
- Tránh sử dụng FTP đơn thuần khi truy cập vào hosting/ VPS của bạn. Hãy sử dụng SSH (SFTP) hoặc FTPS. Giao thức FTP được viết trong thời kỳ “mông muội” của internet và nó không thực sự an toàn để sử dụng ở thời điểm hiện tại.

Tất nhiên, mật khẩu không nên được chia sẻ giữa các người dùng hoặc lưu trữ ở dạng văn bản thuần túy ở bất cứ nơi nào (trên internet hay trên máy tính của bạn). Hãy sử dụng các phần mềm chuyên dụng để lưu trữ chúng.

13. Chỉ cập nhật blog/ website của bạn từ các mạng internet đáng tin cậy

Cập nhật ở đây nên được hiểu với nghĩa rộng hơn là đăng nhập và tiến hành các thao tác chỉnh sửa, đăng tải, update... trên blog/ website của bạn. Nhiều người thường có thói quen sử dụng mạng wifi miễn phí ở các quán cà phê, nhà hàng... để tranh thủ hoàn thành nốt công việc còn dang dở trên blog/ website của mình, bất cứ khi nào có thể. Nhưng bạn biết không, những kết nối wifi mà bạn đang vô tư sử dụng đó có thể không an toàn. Không ít trong số chúng là công cụ tiếp tay cho hacker đánh cắp thông tin đăng nhập của bạn (nếu không được mã hóa).

Vì vậy, hãy cân nhắc kỹ càng trước khi sử dụng các mạng internet công cộng, wifi miễn phí... để cập nhật thông tin trên blog/ website của mình.

14. Sử dụng một phần mềm diệt virus trên máy tính

Đây là yêu cầu gần như bắt buộc nếu bạn muốn đảm bảo cả máy tính lẫn blog/ website của bạn được an toàn. Virus và phần mềm độc hại hoàn toàn có thể lây lan từ máy tính của bạn vào blog/ website thông qua trình duyệt web. Hãy thử nghĩ xem, máy tính của bạn bị nhiễm virus từ các website khác thông qua trình duyệt web. Vậy thì không có lý do gì để chúng không thể làm điều ngược lại phải không nào.

Ngoài ra, virus, trojan, malware, spyware... còn có khả năng đánh cắp thông tin đăng nhập, thông tin thẻ tín dụng, cũng như các thông tin cá nhân khác của bạn.

Do đó, việc cài đặt một phần mềm diệt virus đủ mạnh, có bản quyền, được update thường xuyên là điều nên làm ngay và luôn. [McAfee LiveSafe](#) là một gợi ý sáng giá khi bạn vừa có phần mềm diệt virus bản quyền dùng không giới hạn số máy tính, vừa có Intel True Key lưu không giới hạn số lượng mật khẩu.

15. Kích hoạt Google Search Console

Nếu bạn nghĩ Google Search Console hay Google Webmaster Tools chỉ có chức năng duy nhất là hỗ trợ SEO thì chắc chắn bạn đã nhầm. Ngoài việc quản lý việc index dữ liệu blog/ website, Google Search Console còn đảm nhận cả chức năng theo dõi uptime cũng như vấn đề bảo mật của chúng.

Chỉ cần Google bots phát hiện thấy blog/ website của bạn bị down trong thời gian quá lâu hoặc dính mã độc, ngay lập tức, bạn sẽ nhận được thông báo qua email. Những cảnh báo này thường rất chính xác và chúng chỉ mất khi bạn xác nhận với Google rằng vấn đề đã được xử lý. Họ sẽ kiểm tra lại để chắc chắn trước khi gỡ bỏ cảnh báo.

Google

Search Console

Dashboard

Messages

▸ Search Appearance ⓘ

▸ Search Traffic

▸ Google Index

▸ Crawl

Security Issues

Other Resources

Security Issues

! Harmful content

Google has detected harmful content on some of your site's pages. We rec...
Google Chrome will display a warning when users visit or download certain f...

Download all samples

Malicious content Sample

These pages contained harmful content. Unfortunately, the malicious code within the page could not be isolated.

[Show details](#)

I have fixed these issues

REQUEST A REVIEW

Google Search Console mang lại rất nhiều lợi ích. Vậy nên, đừng bao giờ quên thiết lập nó cho blog/ website của bạn nhé.

16. Bảo vệ WordPress bằng một plugin bảo mật

Giống như hệ điều hành máy tính cần phần mềm diệt virus, blog/ website WordPress cũng cần một plugin bảo mật đủ mạnh để đảm bảo nó an toàn. Những plugin bảo mật được chúng tôi đánh giá cao bao gồm:

- [Sucuri Security](#)
- [Wordfence Security](#)
- [iThemes Security](#)
- [All In One WP Security & Firewall](#)

Riêng với plugin Sucuri Security, *WP Căn bản* đã có hẳn 1 bài viết hướng dẫn chi tiết cách cài đặt và sử dụng. Các bạn có nhu cầu có thể tham khảo thêm [tại đây](#).

17. Thường xuyên sao lưu dữ liệu của blog/ website

Cứu cánh cuối cùng giúp bạn khôi phục blog/ website về trạng thái ban đầu khi các phòng tuyến khác đều đã thất thủ là thường xuyên sao lưu dữ liệu. Có 4 giải pháp khác nhau để làm việc này, bao gồm:

- Sao lưu bằng các plugin như [BackUpWordPress](#), [BackWPup](#), [UpdraftPlus](#)... Danh sách các plugin hỗ trợ backup phổ biến khác, các bạn có thể tham khảo thêm [tại đây](#).
- Sao lưu bằng dịch vụ trả phí của bên thứ 3 như [VaultPress](#), [BlogVault](#)... WP Căn bản đang sử dụng dịch vụ của VaultPress và cảm thấy rất hài lòng.
- Sao lưu thủ công: trích xuất mã nguồn và database của blog/ website về lưu trữ trên máy tính. Các bạn có thể tham khảo hướng dẫn chi tiết [tại đây](#).
- Sao lưu bằng cách dịch vụ backup được tích hợp sẵn trong hosting, chẳng hạn như [R1Soft Backup](#), [JetBackup](#)... Chúng thường sao lưu tự động và bạn không thể lựa chọn dữ liệu backup hay thiết lập tần suất backup.

Các bạn nên sử dụng kết hợp ít nhất 2 trong số 4 giải pháp kể trên để đảm bảo dữ liệu luôn an toàn. Tuy nhiên, không nên quá lạm dụng chúng, cũng không nên thiết lập tần suất backup quá dày để tránh ảnh hưởng đến tài nguyên của host. Tần suất backup hợp lý là từ 1 đến 2 lần/ ngày nếu dữ liệu blog/ website của bạn thường xuyên thay đổi.

18. Thường xuyên kiểm tra danh sách người dùng

Đây là một lời khuyên nghe có vẻ thừa nhưng lại không thừa. Bạn nên thường xuyên kiểm tra danh sách tài khoản người dùng trên blog/ website của mình. Bởi vì hacker hoàn toàn có thể sử dụng các công cụ spam để đăng ký tài khoản bất hợp pháp trên blog/ website của bạn, ngay cả khi bạn đã tắt chức năng cho phép người dùng đăng ký tài khoản mới.

Username	Name	Email	Role	Posts
<input type="checkbox"/>	Trung Hiếu Bùi		Administrator	808
<input type="checkbox"/>	Đức Ngọc Phạm		Subscriber	5
<input type="checkbox"/>	Phước Đt		Subscriber	1
<input type="checkbox"/>	Subiz		Subscriber	1
<input type="checkbox"/>	Thế Khoa Vũ		Subscriber	3

Và mọi việc sẽ trở nên hết sức nguy hiểm nếu tài khoản của hacker có role là Administrator hoặc Editor. Điều đó có nghĩa là chúng hoàn toàn có quyền sinh sát đối với blog/ website của bạn. Tôi đã từng phải giải quyết trường hợp tương tự cho một khách hàng. Bằng cách nào đó, hacker đã tạo tài khoản Administrator trên website của anh ta, sau đó upload và cài đặt các plugin có chứa công cụ phát tán mã độc lên site.

Do đó, thường xuyên kiểm tra danh sách người dùng, loại bỏ những tài khoản đáng ngờ và thiết lập lại role cho hợp lý là việc cần thiết để bảo vệ an toàn cho blog/ website của bạn.

PHẦN II. CÁC THỦ THUẬT BẢO MẬT WORDPRESS CĂN BẢN

19. Cài đặt SSL cho blog/ website

Như đã nói ở mục 12, cài đặt SSL (HTTPS) cho blog/ website của bạn là một trong những bước quan trọng để đảm bảo nó luôn an toàn. Các tập tin, dữ liệu được truyền tải từ trình duyệt web của người dùng đến máy chủ và ngược lại sẽ được mã hóa theo cách mà chỉ có “chính chủ” mới có thể giải mã được. Điều này giúp bảo vệ dữ liệu khỏi sự theo dõi của hacker. Nó cũng giúp blog/ website của bạn tránh được các cuộc tấn công thay đổi giao diện thông qua việc chèn thêm file bất hợp pháp vào mã nguồn.

SSL cũng là một trong những yếu tố được Google và các cỗ máy tìm kiếm khác dùng làm thước đo để xếp hạng kết quả tìm kiếm. Nghĩa là những trang sử dụng giao thức HTTPS sẽ được Google ưu tiên hơn một chút. Cài SSL cũng làm tăng mức độ uy tín của blog/ website với người dùng. Họ sẽ bớt e ngại hơn khi đăng nhập hay gửi thông tin cá nhân trên blog/ website của bạn.

Vì vậy, bất cứ khi nào có điều kiện, các bạn nên cài đặt SSL cho blog/ website của mình.

Hai loại SSL phổ biến và đủ dùng hiện nay là Let's Encrypt (miễn phí) và PositiveSSL (trả phí, giá rẻ).

- Let's Encrypt thường được phần lớn các nhà cung cấp hosting tích hợp sẵn trong cPanel và các bạn có thể kích hoạt nó một cách nhanh chóng chỉ với vài thao tác đơn giản. Ví dụ như với hosting của HawkHost, StableHost... các bạn có thể làm theo hướng dẫn [sau đây](#). Còn [đây](#) là bài viết tham khảo dành cho các bạn đang dùng VPS.
- PositiveSSL của Comodo là một trong những loại SSL trả phí thuộc hàng rẻ nhất. Giá chỉ khoảng \$10/năm. Nếu bạn muốn giá rẻ hơn, có thể mua tại [NameCheap](#) với giá chỉ khoảng \$3/năm. Quy trình cài PositiveSSL có phức tạp hơn Let's Encrypt một chút, nhưng nhìn chung cũng khá đơn giản. Hướng dẫn chi tiết, các bạn có thể xem [tại đây](#).

Các bạn cũng có thể cài SSL miễn phí của CloudFlare nếu blog/ website của bạn đang sử dụng dịch vụ CDN này. Tuy nhiên, điểm yếu của loại SSL này là không tương thích với các trình duyệt web phiên bản cũ. Vậy nên, các bạn cần cân nhắc kỹ trước khi sử dụng. Hướng dẫn chi tiết vui lòng xem [tại đây](#).

Sau khi cài SSL thành công, việc còn lại của các bạn là cấu hình để chuyển blog/ website sang giao thức HTTPS. Tham khảo các bài viết sau đây sẽ giúp bạn dễ dàng làm được điều đó:

- [Cài SSL cho WordPress trong nháy mắt với plugin Really Simple SSL](#)
- [Hướng dẫn chuyển từ HTTP sang HTTPS không bị mất thứ hạng](#)
- [Cấu hình HSTS cho blog/ website thông qua file .htaccess](#)

20. Hạn chế số lần đăng nhập thất bại

Đây là thủ thuật giúp bạn chống lại brute force attack. Như đã nói ở các mục 9 và 10, hacker sẽ sử dụng công cụ để dò tên đăng nhập và mật khẩu của bạn bằng cách thử đi, thử lại nhiều lần với các chuỗi bất kỳ. Một trong những cách hiệu quả nhất để chống lại phương thức tấn công này là giới hạn số lần đăng nhập thất bại. Nghĩa là một địa chỉ IP nào đó sẽ bị cấm đăng nhập tạm thời (trong khoảng thời gian nhất định) hoặc vĩnh viễn nếu người dùng IP đó đăng nhập sai vượt quá số lần quy định.

Trong WordPress, các bạn có thể làm điều này một cách dễ dàng nhờ sự trợ giúp của một số plugin chuyên dụng như [Login LockDown](#), [Limit Login Attempts](#) hay [WP Limit Login Attempts](#).

Login LockDown Options

Settings Activity (0)

Max Login Retries

Number of failed login attempts within the "Retry Time Period Restriction" (defined below) needed to trigger a LockDown.

3

Retry Time Period Restriction (minutes)

Amount of time that determines the rate at which failed login attempts are allowed before a LockDown occurs.

5

Lockout Length (minutes)

How long a particular IP block will be locked out for once a LockDown has been triggered.

60

Lockout Invalid Usernames?

By default Login LockDown will not trigger if an attempt is made to log in using a username that does not exist. You can override this behavior here.

Yes No

Mask Login Errors?

WordPress will normally display distinct messages to the user depending on whether they try and log in with an invalid username, or with a valid username but the incorrect password. Toggling this option will hide why the login failed.

Yes No

Show Credit Link?

By default, Login LockDown will display the following message on the login form:

Login form protected by [Login LockDown](#).

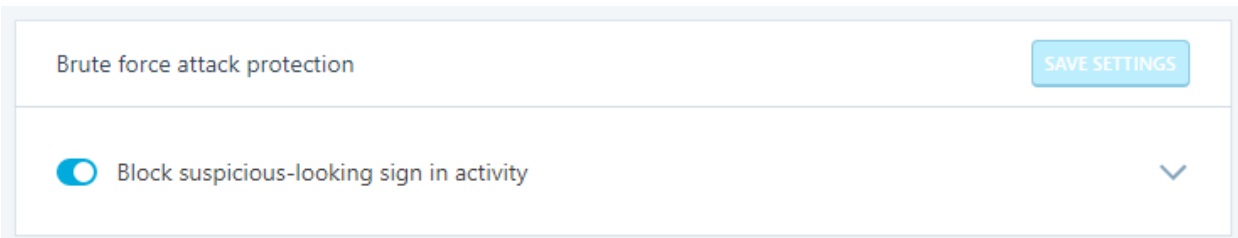
This helps others know about the plugin so they can protect their blogs as well if they like. However, you can disable this message if you prefer.

Yes, display the credit link.
 Display the credit link, but add "rel='nofollow'" (ie. do not pass any link juice).
 No, do not display the credit link.

Update Settings

Những plugin bảo mật như Sucuri Security cũng có sẵn tính năng này, nên nếu bạn đã cài Sucuri theo hướng dẫn ở mục 16 thì không cần thiết phải cài thêm plugin khác nữa. Phần thiết lập này nằm trong tab *Last Logins => Failed Logins* và *Blocked Users*.

Module [Protect](#) của plugin Jetpack cũng có chức năng tương tự nên nếu bạn đang dùng Jetpack thì có thể tận dụng luôn. Truy cập *Jetpack => Settings => Security* và kích hoạt mục *Block suspicious-looking sign in activity* lên là được.



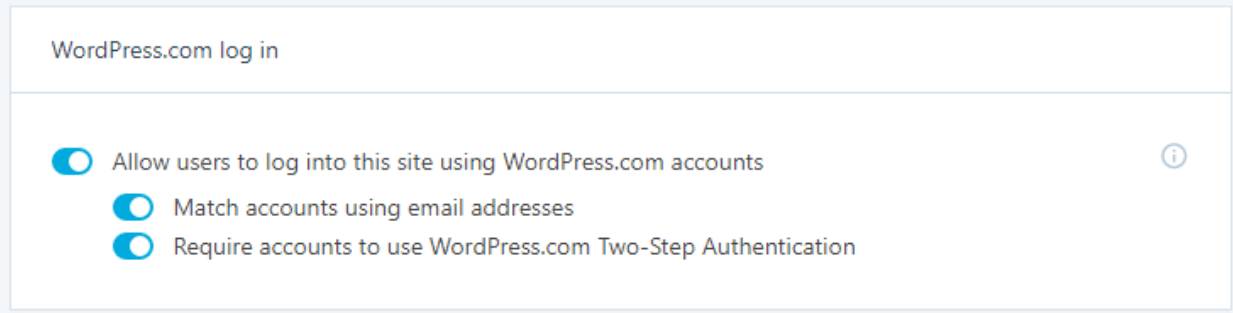
21. Kích hoạt xác thực hai nhân tố (bảo mật 2 bước)

Thủ thuật này nên được áp dụng trên cả trang đăng nhập WordPress lẫn trang đăng nhập cPanel của hosting (nếu nhà cung cấp hosting có hỗ trợ). Hiểu một cách đơn giản, nếu muốn đăng nhập vào blog/ website WordPress hay cPanel, ngoài việc nhập tên và mật khẩu thông thường, người dùng sẽ phải nhập thêm một dãy số được tạo bất kỳ từ ứng dụng của bên thứ 3 (thông dụng nhất là Google Authenticator).

Nó có thể giúp blog/ website của bạn an toàn ngay cả khi hacker dò được tên đăng nhập và mật khẩu chính xác. Bởi vì một dãy số của Google Authenticator chỉ tồn tại trong vòng 30 giây, sau đó sẽ tự động đổi sang dãy số khác.

Để kích hoạt tính năng xác thực 2 nhân tố trên blog/ website WordPress, các bạn có thể sử dụng plugin [Google Authenticator](#). Hướng dẫn chi tiết, các bạn có thể xem [tại đây](#).

Nếu bạn đang sử dụng plugin Jetpack, bạn hoàn toàn có thể kích hoạt module Single Sign On trong Jetpack => Settings => Security => WordPress.com log in để đăng nhập bằng tài khoản WordPress.com và sử dụng tính năng xác thực 2 nhân tố.



Tham khảo thêm:

- [Bật tính năng bảo mật 2 bước cho tài khoản WordPress.com](#)
- [Đăng nhập WordPress thông qua tài khoản WordPress.com](#)

Tương tự đối với cPanel, các bạn nên bật tính năng xác thực 2 nhân tố ngay nếu nhà cung cấp hosting có hỗ trợ. Tham khảo bài viết [sau đây](#) để làm điều đó một cách dễ dàng.

22. Bảo đảm chính xác quyền của tập tin và thư mục

Quyền của tập tin và thư mục hay còn gọi là permission. PHP và WordPress nói chung sử dụng một tập hợp các quyền liên quan đến các tập tin và thư mục. Nếu không đi sâu vào chi tiết, có một số loại quyền cơ bản sau đây:

- Các tập tin và thư mục có thể ghi công khai
- Các tập tin chỉ được ghi bởi máy chủ web
- Các tập tin chỉ đọc
















Nói chung, máy chủ web của bạn thường cần có quyền viết các tập tin cho WordPress để chúng có thể hoạt động chính xác. Trong khi các đối tượng khác không nên có quyền ghi vào tập tin của bạn.

Một số nhà phát triển thiếu kinh nghiệm hoặc lười biếng, có thể đề nghị bạn thay đổi quyền truy cập sang mức lỏng lẻo hơn. Ví dụ, họ có thể đề xuất làm cho một số tập tin hoặc thư mục công khai ghi được (777). Điều này sẽ tạo ra một mối đe dọa an ninh nghiêm trọng bởi vì nó có nghĩa là bất cứ ai cũng có thể viết bất cứ điều gì vào thư mục hay tập tin đó. Họ cũng có thể tìm cách để nhảy ra khỏi thư mục và gây ra sự tàn phá trên phần còn lại của blog/ website.

Theo nguyên tắc chung, các tập tin nên được thiết lập quyền là 644 và các thư mục là 755. Riêng tập tin `wp-config.php` nên có quyền truy cập là 400 hoặc 440.

Làm thế nào để kiểm tra xem liệu quyền của các tập tin và thư mục đã chính xác hay chưa? Cách thứ nhất là truy cập vào File Manager của cPanel/ DirectAdmin để kiểm tra và chỉnh sửa permission theo phương pháp thủ công.

Home Up One Level Back Forward Reload Select All Unselect All View Trash Empty Trash

Name	Size	Last Modified	Type	Permissions
 index.php	418 bytes	Jun 8, 2016 3:37 PM	application/x-httpd-php	0644
 license.txt	19.47 KB	Jun 8, 2017 10:34 PM	text/plain	0644
 readme.html	7.24 KB	Jun 8, 2017 10:34 PM	text/html	0644
 robots.txt	258 bytes	Mar 5, 2017 11:36 PM	text/plain	0644
 wp-activate.php	5.32 KB	Dec 7, 2016 7:50 AM	application/x-httpd-php	0644
 wp-blog-header.php	364 bytes	Jun 8, 2016 3:37 PM	application/x-httpd-php	0644
 wp-comments-post.php	1.59 KB	Dec 7, 2016 7:50 AM	application/x-httpd-php	0644
 wp-config-sample.php	2.79 KB	Jun 8, 2016 3:37 PM	application/x-httpd-php	0644
 wp-config.php	3.62 KB	Mar 15, 2017 1:12 PM	application/x-httpd-php	0644
 wp-cron.php	3.21 KB	Jun 8, 2016 3:37 PM	application/x-httpd-php	0644
 wp-links-opml.php	2.37 KB	Dec 7, 2016 7:50 AM	application/x-httpd-php	0644
 wp-load.php	3.22 KB	Dec 7, 2016 7:50 AM	application/x-httpd-php	0644
 wp-login.php	33.52 KB	Jun 8, 2017 10:34 PM	application/x-httpd-php	0644
 wp-mail.php	7.86 KB	Jan 12, 2017 3:35 AM	application/x-httpd-php	0644
 wp-settings.php	15.82 KB	Jun 8, 2017 10:34 PM	application/x-httpd-php	0644

Cách thứ 2 là sử dụng plugin [Defender](#) (trả phí) để kiểm tra và sửa các quyền truy cập tập tin hoàn toàn tự động.

SCAN REPORTS SHOW LOG

RUNNING NEW SCAN

This scan is running in the background and will continue to run if you navigate away or close your browser. Check back in a few minutes to see your results.

53.77%

Analyzing wp-content files...

[CANCEL SCAN](#)

Nếu kinh phí quá eo hẹp, các bạn có thể xem xét mua plugin này thông qua chương trình “[mua chung](#)” của WP Căn bản với giá chỉ 150.000 VNĐ/năm.

23. Thay đổi tiền tố bảng mặc định của database

Đây là tàn dư của các phiên bản WordPress cũ. Trước đây, tên của các bảng trong cơ sở dữ liệu (database) của WordPress thường được bắt đầu với tiền tố wp_

The screenshot shows the database management interface for a WordPress installation. On the left, there is a sidebar with a 'Database' section containing a dropdown menu set to '_wordpress (11)'. Below it, a tree view shows the database structure for 'monzilla_wordpress (11)', listing various tables like wp_commentmeta, wp_comments, wp_links, etc. The main area displays a table with columns 'Table' and 'Action'. The 'Table' column lists 11 tables, all starting with 'wp_'. A red box highlights the 'wp_' prefix in the first few rows. The 'Action' column contains icons for editing, deleting, and other operations. At the bottom, it shows '11 table(s)' and a 'Sum' button.

Table	Action
<input type="checkbox"/> wp_commentmeta	[Icons]
<input type="checkbox"/> wp_comments	[Icons]
<input type="checkbox"/> wp_links	[Icons]
<input type="checkbox"/> wp_options	[Icons]
<input type="checkbox"/> wp_postmeta	[Icons]
<input type="checkbox"/> wp_posts	[Icons]
<input type="checkbox"/> wp_terms	[Icons]
<input type="checkbox"/> wp_term_relationships	[Icons]
<input type="checkbox"/> wp_term_taxonomy	[Icons]
<input type="checkbox"/> wp_usermeta	[Icons]
<input type="checkbox"/> wp_users	[Icons]
11 table(s)	Sum

Mặc dù hiện nay, nó không còn là thiết lập mặc định nữa, nhưng một số người vẫn có xu hướng... hoài cổ và các phiên bản WordPress cũ hơn vẫn phải sống chung với lũ. Chính vì sự phổ biến của nó, nên hacker đã dễ dàng thực hiện các cuộc tấn công SQL injection vào database WordPress nhờ biết trước tiền tố bảng.

Vì vậy, nếu bạn đang sử dụng tiền tố bảng mặc định là wp_ trong database thì nên nhanh chóng thay đổi chúng để đảm bảo an toàn cho blog/ website. Có 2 cách để thay đổi tiền tố bảng cho database:

Với phương pháp tự động, các bạn sẽ cần phải sử dụng plugin [Change Table Prefix](#), All In One WP Security & Firewall hoặc iThemes Security.

Tất cả những gì các bạn cần làm là cài đặt và kích hoạt plugin Change Table Prefix. Sau đó, truy cập vào *Settings* => *Change Table Prefix* => Tích vào mục *Would you like to your own custom prefix* => Điền tiền tố mà bạn muốn thay vào khung, sau đó click nút *Click To Change Table Prefix* là xong.

Wordpress Database Table Prefix Changing

This plugin will change your site database table prefix to protect from SQL Injection attacks.

Your current table prefix is: wp_

Your next table prefix will be random generated 5 characters long alpha string followed by underscore(_) if below checkbox unchecked.

Warning: Please make sure to take backup of your site database and wp-config.php file is in writable mode before start table prefix change.

Enable site as maintenance mode

Would you like to your own custom prefix.

wpcb

Với những bạn thích sự phức tạp, có thể tham khảo [bài viết này](#) (tiếng Anh).

24. Đảm bảo bạn đã đặt khóa xác thực WordPress bí mật

Bạn có thể đã từng nhìn thấy tám khoá bảo mật và xác thực WordPress trong tập tin *wp-config.php* của mình và tự hỏi chúng là gì? Bạn cũng có thể chưa bao giờ nhìn thấy hoặc nghe nói về chúng.

Chúng trông giống như sau:

```
define('AUTH_KEY',          'R*:M|{:DdK-.MwX08dfDrc?20.zwnXV.UEBN#zN #<88nFwCZ)c-M7P3;@/D0!Pz');
define('SECURE_AUTH_KEY',  'kr+b,UXz-aZ1h*|,f!Ceb#XO>LfZ[?8e1PKw_nWqV*T`cp#_8S2vOy%=Eps$h7P1');
define('LOGGED_IN_KEY',    '~S4G_MD=w.M;j4^0 [q%K7uaR-_];t E7W(MWm 0eXF3nU:opRZR0k/pk:JJCd_e');
define('NONCE_KEY',        '.x,];tKYZUT:6n(gr?j|(1xt3g8cB4@8TB3~$~i1),7jW0%RyE+st4JB}_UW}B_a');
define('AUTH_SALT',        '4w>XmXpVp~;MG]?4+Y;n![ME:e8B]vAi|Q|5[j[0S~rfep}2]P?O&/9A1y[mWsaJ');
define('SECURE_AUTH_SALT', '^Zq|XCZ.<@j|Z#XX]~b.Kf!cvf5VxfHMZw!k;G[[K^DIpNi^/h`Z<;ZM1E ?C#8/');
define('LOGGED_IN_SALT',   '0k:1+x@F1?fwI[$k#|#ey$U-GhZ=-C_/Fz|zXws/]ba]Y;b4-x%1$}{ QM)9T1(a');
define('NONCE_SALT',       ']4D%#d8A{TPj#@j&9a99R-y>T+V|Sg=-NH*$_ddNk6r}c3BxEP`cvUIb_0xs+slw4');
```

Về cơ bản, đây là các biến ngẫu nhiên được sử dụng để làm cho mật khẩu đăng nhập WordPress của bạn khó đoán hoặc crack. Sở dĩ như vậy là bởi vì nó gán thêm một phần tử ngẫu nhiên vào cách mà mật khẩu được lưu trữ trong cơ sở dữ liệu của bạn, làm cho hacker gặp nhiều khó khăn hơn khi tấn công theo phương thức brute force.

Hầu hết các blog/ website WordPress tự cài đặt thủ công (không phải cài qua các ứng dụng của bên thứ 3 như Softaculous) đều mặc định không có khóa xác thực trong file *wp-config.php*. Do đó, tất cả những gì bạn cần làm bây giờ là:

- Truy cập vào [WordPress Security Key Generator](#). Copy toàn bộ 8 khóa xác thực.
- Mở file *wp-config.php* của bạn ra, paste đè lên phần còn trống tương ứng với 8 khóa bảo mật, sau đó lưu lại.

Thủ thuật này nên được lặp lại mỗi tháng 1 lần để đảm bảo an toàn cho blog/ website của bạn.

25. Vô hiệu hóa thực thi tập tin PHP

Một trong những điều đầu tiên hacker sẽ làm nếu chúng có quyền truy cập vào blog/ website của bạn là thực thi các file PHP từ trong một thư mục trên hosting. Nhưng nếu bạn tắt tính năng thực thi tập tin PHP, ngay cả khi một lỗ hổng bảo mật tồn tại trên blog/ website, sự bảo vệ này sẽ làm tê liệt phần còn lại của nỗ lực tiếp cận mục tiêu của hacker.

Đây là lớp phòng vệ mạnh mẽ của WordPress và có thể phá vỡ chức năng của một số theme hoặc plugin cần thiết. Nhưng bạn nên thực hiện thủ thuật này ít nhất trong các thư mục dễ bị tổn thương như *wp-includes* và *uploads*.

Tạo file *.htaccess* trong thư mục *wp-includes* và thêm đoạn code sau đây vào nội dung của nó.

```
<Files *.php>
deny from all
</Files>
<Files wp-tinymce.php>
allow from all
</Files>
<Files ms-files.php>
allow from all
</Files>
```

Tạo file *.htaccess* trong thư mục *wp-content/uploads* và thêm đoạn code sau đây vào nội dung của nó.

```
<Files *.php>
deny from all
</Files>
```

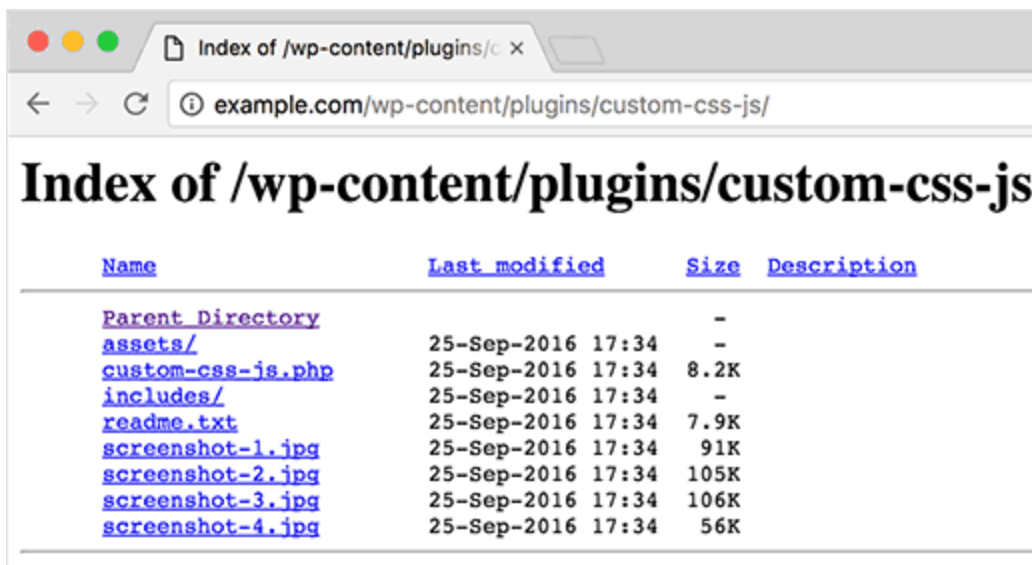
Bạn cũng có thể làm điều tương tự với thư mục *wp-content* nếu nó không gây ảnh hưởng đến chức năng của theme và plugin.

Nếu bạn đã cài đặt plugin Sucuri ở mục 16, bạn có thể bỏ qua mục này.

Lưu ý: Nếu bạn không thấy file *.htaccess* hiển thị trên File Manager, ngay cả khi đã tạo file mới, hãy làm theo hướng dẫn [sau đây](#).

26. Vô hiệu hóa “directory indexing và browsing”

Directory browsing (trình duyệt thư mục) có thể được sử dụng bởi hacker để tìm ra các lỗ hổng trong tập tin mã nguồn của bạn. Bởi vì họ có thể xem được danh sách các tập tin này và truy cập chúng.



Directory browsing cũng có thể được sử dụng bởi những người khác để xem các tập tin của bạn, sao chép hình ảnh, tìm ra cấu trúc thư mục của bạn và các thông tin liên quan. Đây là lý do tại sao bạn nên tắt directory indexing và browsing trên hosting của mình.

Để làm điều này, đơn giản chỉ cần thêm đoạn code sau đây vào trong các file `.htaccess` mà các bạn đã tạo ở mục 25 rồi lưu lại là xong.

Options All -Indexes

27. Phân tách cơ sở dữ liệu WordPress của bạn

Nếu bạn chạy nhiều blog/ website trên cùng một tài khoản hosting, bạn có thể bị cám dỗ để rời tạo ra tất cả các blog/ website trong cùng một cơ sở dữ liệu (WordPress multi-site). Điều này tạo ra một nguy cơ bảo mật cho WordPress. Nếu một trang bị xâm nhập, tất cả các trang khác được lưu trữ trên cùng một cơ sở dữ liệu cũng có nguy cơ bị hacker tấn công.

Khi cài đặt WordPress, điều đầu tiên bạn cần làm là tạo một cơ sở dữ liệu hoàn toàn mới. Cung cấp cho nó một tên cơ sở dữ liệu, tên người dùng cơ sở dữ liệu và mật khẩu riêng biệt, khác với bất kỳ blog/ website nào mà bạn đã tạo trước đó.

Bằng cách này, nếu một trong các blog/ website của bạn bị tấn công, mã độc hoặc virus sẽ không lan sang các trang khác của bạn trên cùng một tài khoản shared hosting.

28. Hạn chế quyền của người dùng cơ sở dữ liệu

Khi cài đặt một blog/ website WordPress lần đầu tiên, bạn có thể vì thiếu thông tin, đã vô tình tạo ra một vấn đề bảo mật thông qua các đặc quyền dành cho người dùng cơ sở dữ liệu (database users). Theo thói quen, hầu như tất cả mọi người đều chọn ALL PRIVILEGES khi cấp quyền truy cập database cho database user.

Đối với hầu hết các hoạt động hàng ngày của WordPress, người dùng cơ sở dữ liệu chỉ cần đọc dữ liệu và các đặc quyền cho phép ghi dữ liệu vào database như: SELECT, INSERT, UPDATE và DELETE.

Do đó, bạn có thể loại bỏ các đặc quyền bổ sung, như: DROP, ALTER và GRANT để nâng cao khả năng bảo mật database.

Để thay đổi quyền cho người dùng database, với hosting cPanel, các bạn truy cập *MySQL® Databases* => Click vào tên người dùng database mà bạn muốn chỉnh sửa phân quyền (trong cột *Privileged Users*) => Bỏ dấu tích trong các quyền không cần thiết và click nút *Make Changes* để lưu lại.

Manage User Privileges

User:

Database:

ALL PRIVILEGES

ALTER ALTER ROUTINE

CREATE CREATE ROUTINE

CREATE TEMPORARY TABLES CREATE VIEW

DELETE DROP

EVENT EXECUTE

INDEX INSERT

LOCK TABLES REFERENCES

SELECT SHOW VIEW

TRIGGER UPDATE

Lưu ý: Một số nâng cấp lớn của WordPress có thể thực sự cần những đặc quyền này, tuy nhiên trong hầu hết các trường hợp, việc hoạt động của WordPress không cần đến chúng và bạn có thể tắt chúng đi.

29. Vô hiệu hoá chỉnh sửa tập tin từ bảng quản trị WordPress

Khi đang trong giai đoạn đầu của việc xây dựng một blog/ website, có thể bạn sẽ cần phải chỉnh sửa các tập tin theme và plugin rất nhiều. Theo mặc định, quản trị viên có quyền chỉnh sửa các tập tin PHP và CSS ngay trong bảng quản trị của WordPress, thông qua mục *Editor* của *Plugins* hay *Appearance*.

Khi blog/ website đã được phát triển hoàn tất và hoạt động ổn định, bạn sẽ không cần phải chỉnh sửa những tập tin này nữa. Đây chính là lúc bạn cần vô hiệu hóa tính năng cho phép chỉnh sửa file theme và plugin từ trong WordPress Dashboard.

Bởi vì, việc cho phép các quản trị viên chỉnh sửa tập tin là một vấn đề bảo mật khá nghiêm trọng. Nếu một hacker có quyền đăng nhập vào blog/ website của bạn với role Administrator, chúng sẽ ngay lập tức chèn các đoạn mã độc vào trong file theme/ plugin thông qua tính năng này.

Chèn đoạn code sau đây vào file *wp-config.php* và lưu lại.

```
define('DISALLOW_FILE_EDIT', true);
```

Khi cần chỉnh sửa file theme/ plugin, các bạn chỉ cần bỏ code bên trên khỏi file *wp-config.php* là được. Hoặc truy cập và chỉnh sửa thông qua File Manager của cPanel/ DireAdmin và phần mềm FTP.

30. Bảo vệ tập tin wp-config.php của bạn

Nếu mã nguồn WordPress của bạn tương tự như cơ thể con người thì tập tin *wp-config.php* chính là trái tim của nó. Tập tin *wp-config.php* có chứa tất cả các thông tin quan trọng của WordPress như:

- Tên database, database user, database password.
- Các khóa xác thực và bảo mật
- Tên tiền tố bảng của database
- Nhiều thiết lập quan trọng khác

Không ít code mà bạn sử dụng từ đầu ebook đến giờ đều được chèn vào file *wp-config.php*. Do vậy, bảo vệ file *wp-config.php* là nhiệm vụ tối quan trọng nếu bạn muốn đảm bảo blog/ website của mình an toàn.

Ngoài việc thiết lập permission là 400 hoặc 440 hoặc chí ít là 644 như ở mục 22, các bạn nên thêm code sau đây vào trên cùng của file *.htaccess* ở thư mục gốc của WordPress (nằm ngang hàng với file *wp-config.php*).

```
<files wp-config.php>
order allow,deny
deny from all
</files>
```


Nếu một plugin nào đó yêu cầu được viết vào file *wp-config.php* (chẳng hạn các plugin tạo cache), các bạn buộc phải chuyển permission về 644, đồng thời gỡ bỏ code bên trên ra khỏi file *.htaccess* thì plugin mới có thể viết được.

31. Bảo vệ tập tin *.htaccess* của bạn

Tập tin *.htaccess* mà bạn vừa chèn code bảo vệ file *wp-config.php* ở mục 30 cũng chính là một đối tượng nằm trong danh sách cần được bảo vệ. Nó là nơi chứa code giúp bạn tạo pretty permalinks (cấu trúc đường dẫn chuẩn SEO như nhiều người vẫn thường gọi), cache dữ liệu, nén dữ liệu tĩnh, redirect từ link cũ sang link mới, redirect từ link HTTP sang HTTPS...

Do đó, nếu không may hacker chiếm được quyền kiểm soát file này, chúng có thể chuyển hướng blog/ website của bạn tới địa chỉ mà chúng mong muốn.

Để bảo vệ file *.htaccess* trong thư mục gốc của WordPress, những gì các bạn cần làm là thêm code sau đây vào bên trong chính nó.

```
<Files .htaccess>
order allow,deny
deny from all
</Files>
```

Và cũng giống như file *wp-config.php*, code bên trên cần phải được loại bỏ trước khi một plugin nào đó có thể viết nội dung vào file *.htaccess*.

32. Vô hiệu hoá XML-RPC (nếu bạn không sử dụng nó)

WordPress sử dụng XML-RPC để cho phép người dùng thực hiện nhiều hoạt động trên blog/ website của họ từ xa. Nó cho phép bạn truy cập vào blog/ website của mình bằng cách sử dụng các ứng dụng di động dành riêng cho WordPress. Với XML-RPC, bạn có thể đăng một bài viết trên blog (từ xa) một cách dễ dàng. Chúng cũng được sử dụng để tạo trackback và pingback, cho phép bạn liên kết trang web của mình đến các trang web thú vị khác. Tuy nhiên, nhiều cuộc tấn công WordPress hiện nay đang khai thác các tính năng của XML-RPC để chiếm quyền truy cập vào các blog/ website. Vì vậy, việc vô hiệu hóa các tính năng của XML-RPC (nếu bạn không sử dụng tới) là một ý tưởng không hề tồi để tăng cường khả năng bảo mật cho WordPress.

Bạn có thể sử dụng các plugin như [Disable XML-RPC](#), [Manage XML-RPC](#) hay [Disable XML-RPC Pingback](#) để vô hiệu hóa XML-RPC một cách đơn giản.

Nếu không phải là tín đồ của plugin, bạn có thể vô hiệu hóa XML-RPC thông qua file *.htaccess* trong thư mục gốc của WordPress:

```
<files xmlrpc.php>
order allow,deny
deny from all
</files>
```

Lưu ý: nếu bạn đang sử dụng các plugin như Jetpack trên blog/ website của mình thì bạn không được phép tắt XML-RPC vì Jetpack sẽ không hoạt động được. Để tránh các cuộc tấn công thông qua XML-RPC, các bạn chỉ cần kích hoạt module Protect của Jetpack lên là xong.

33. Vô hiệu hoá thông báo lỗi PHP

Thông thường, tính năng thông báo lỗi PHP (PHP Error Reporting) là một trong những phương pháp hữu hiệu giúp bạn nhanh chóng phát hiện ra các vấn đề về PHP đang tồn tại trên blog/ website của mình và tìm cách khắc phục. Tuy nhiên, nếu bạn để những dòng thông báo này hiển thị công khai trên blog/ website của mình, thì vô tình bạn đang vẽ đường cho hacker tấn công một cách dễ dàng hơn. Ví dụ như trong trường hợp dưới đây, hacker sẽ nhanh chóng phát hiện ra tên đăng nhập tài khoản hosting hoặc VPS của bạn.



Fatal error: Call to undefined function get_header() in /home/toycraft/public_html/blog/content/themes/siteground-wp17/index.php on line 1

This is the website's username

Ngoài ra, các thông báo lỗi PHP cũng sẽ ảnh hưởng không nhỏ đến thẩm mỹ của giao diện và trải nghiệm người dùng. Vì vậy, tốt nhất, bạn nên vô hiệu hóa nó ngay lập tức nếu không có nhu cầu sử dụng.

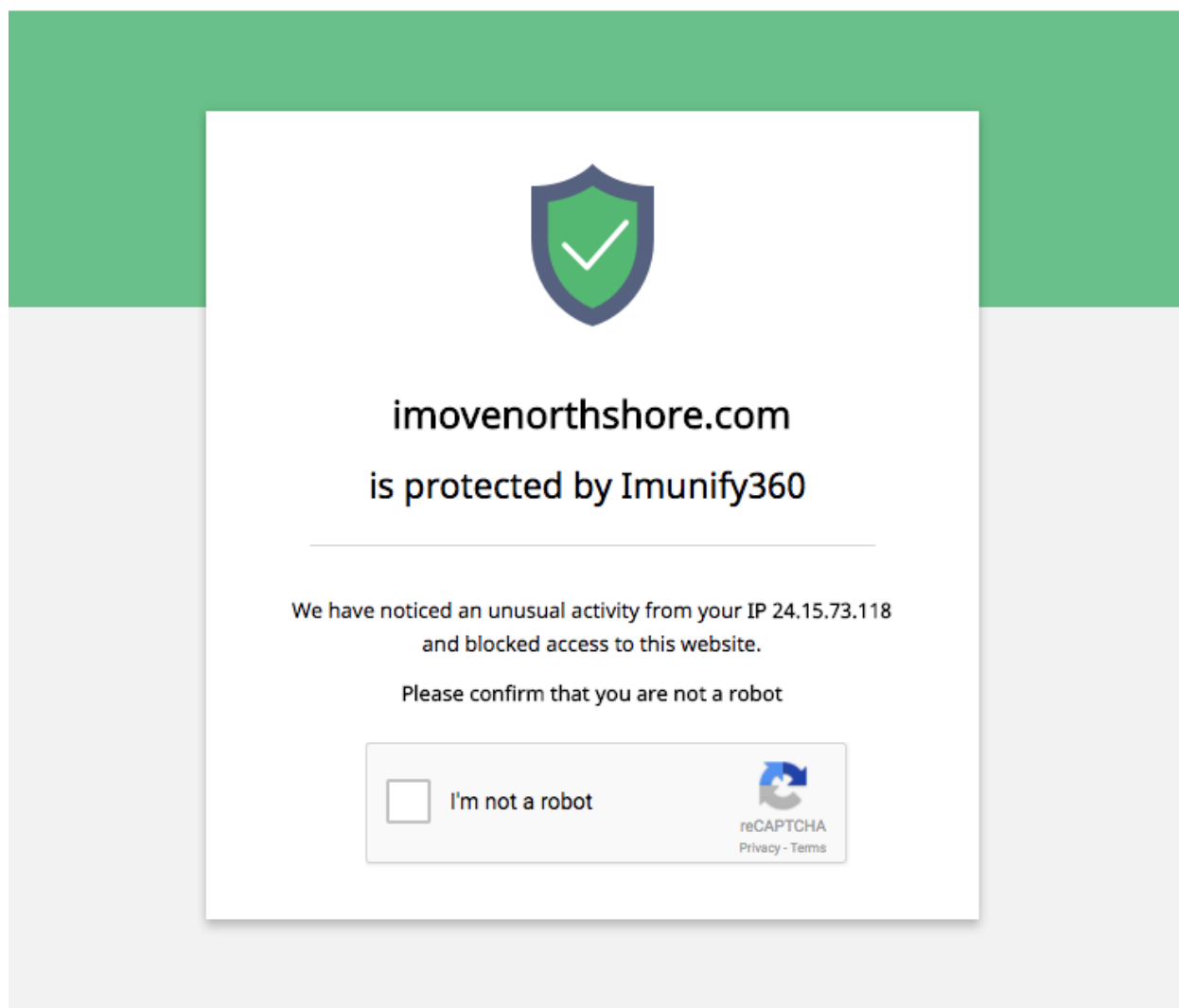
Để vô hiệu hóa thông báo lỗi PHP trong hosting, các bạn có thể tham khảo bài viết [sau đây](#).

34. Cài đặt một tường lửa cho blog/ website

Một bức tường lửa (firewall) có thể được mô tả như một người giữ cửa - bạn chỉ được phép vào một bữa tiệc VIP nếu bạn có mặt trong danh sách khách mời. Giống như người giữ cửa thường ngăn cản người khác xâm nhập, tường lửa có thể được sử dụng để giữ cho hacker không thể đến gần blog/ website của bạn.

Trong trường hợp bảo vệ WordPress, chúng ta sẽ sử dụng một Web Application Firewall (WAF) để giữ cho các hacker không thể sờ mó bàn tay bản thủ vào những nơi mà chúng không có phận sự.

Có rất nhiều WAF khác nhau. Nhưng một trong những tường lửa đáng tin cậy nhất, miễn phí, mã nguồn mở và thường có sẵn trong các dịch vụ hosting là tường lửa ModSecurity.



Bạn có thể kiểm tra xem hosting của mình có hỗ trợ ModSecurity hay không bằng cách truy cập vào cPanel và tìm mục ModSecurity. Nếu có, hãy click vào đó để xem danh sách các blog/website của bạn đang được ModSecurity bảo vệ.

ModSecurity

Configure All Domains

ModSecurity is enabled for all of your domains. You can [Disable](#) ModSecurity for your domains.

Configure Individual Domains

Search

Showing: 10

Domains ▲	Status
[Redacted]	<input checked="" type="button" value="On"/> <input type="button" value="Off"/>
[Redacted] 1	<input checked="" type="button" value="On"/> <input type="button" value="Off"/>
[Redacted] 1	<input checked="" type="button" value="On"/> <input type="button" value="Off"/>
[Redacted]	<input checked="" type="button" value="On"/> <input type="button" value="Off"/>
[Redacted]	<input checked="" type="button" value="On"/> <input type="button" value="Off"/>
[Redacted]	<input checked="" type="button" value="On"/> <input type="button" value="Off"/>
[Redacted]	<input checked="" type="button" value="On"/> <input type="button" value="Off"/>
[Redacted]	<input checked="" type="button" value="On"/> <input type="button" value="Off"/>
wpcanban.com	<input checked="" type="button" value="On"/> <input type="button" value="Off"/>
[Redacted] 1	<input checked="" type="button" value="On"/> <input type="button" value="Off"/>

Một khi nó được kích hoạt, nhà cung hosting của bạn hoặc lập trình viên WordPress đáng tin cậy của bạn thường có thể đề xuất hoặc thực hiện các quy tắc xung quanh ModSecurity.

35. Sử dụng tường lửa của CDN

Chức năng chính của mạng phân phối nội dung (CDN) thường là tối ưu hóa hiệu suất tải blog/ website của bạn từ khắp mọi nơi trên thế giới. Các dịch vụ CDN miễn phí hàng đầu có thể kể đến là [CloudFlare](#) và [Incapsula](#).

Tuy nhiên, các dịch vụ CDN cũng thường cung cấp một tính năng phụ khác và hầu hết trong số chúng có thể bảo vệ blog/ website của bạn chống lại các nguy cơ bảo mật thông qua tường lửa.

Security Level

Adjust your website's Security Level to determine which visitors will receive a challenge page.

This setting was last changed a year ago

Challenge Passage

Specify how long a visitor with a bad IP reputation is allowed access to your website after completing a challenge. After the Challenge Passage TTL expires the visitor in question will have to pass a new Challenge.

This setting was last changed a year ago

Nếu bạn đang sử dụng CDN cho blog/ website WordPress của mình, hãy đảm bảo rằng bạn đã bật các quy tắc bảo mật được cung cấp kèm theo để cải thiện mức độ an toàn cho chúng.

36. Theo dõi lịch sử đăng nhập và các thay đổi của tập tin

Nếu bạn không biết các cuộc tấn công nào đang xảy ra trên blog/ website của mình, bạn hầu như không có khả năng để ngăn chặn chúng, đúng không nào?

Làm thế nào để biết ai đó đang cố gắng đăng nhập vào blog/ website WordPress của bạn? Làm thế nào để biết mã nguồn WordPress của bạn đã bị thay đổi trái phép (chỉnh sửa nội dung hoặc chèn thêm file lạ)? Giải pháp tối ưu nhất là sử dụng một plugin có khả năng theo dõi lịch sử đăng nhập, lịch sử hoạt động của người dùng cũng như lịch sử thay đổi các tập tin.

Sucuri Security được giới thiệu ở mục 16 là một trong những lựa chọn tối ưu nhất để làm điều này. Truy cập *Sucuri Security* => *Settings* => *Enable* mục *Audit Log Statistics*.

Audit Log Statistics

Enabling this option allows you to have a quick view of the range of the activity of your users and/or the attacks directed against your website. By default, the plugin uses the latest 500 entries in the audit logs and uses that information to draw bar and pie charts in the dashboard.

Audit Log Statistics are Enabled Disable

The statistic charts are generated with a limited number of logs stored in the remote API server, you can increase the number to draw the charts with more data and represent the activity during a wider range of days, but you must consider that the bigger the number the slower the plugin dashboard will be because it will take more time to read more logs.

Audit Logs Limit: Save

Sau đó theo dõi lịch sử hoạt động thông qua trang *Dashboard*.

sucuri Sucuri Security
PROTECT YOUR BUSINESS

Dashboard
Malware Scan
Firewall (WAF)
Hardening
Post-Hack
Last Logins
Settings
Site Info

WordPress 4.7.5 is Outdated - Install New Version 4.8 (en_US)

Core Integrity

Every WordPress release comes with a set of files that are part of the standard installation process of each version, none of these files should be modified as they are overwritten on each upgrade, it is not advised that web developers modify the core files and instead extend the base functionality with themes or plugins. Only three directories are scanned: admin, includes, and the document root where the configuration and startup files are located.

Use a [server side scanner](#) or a [web scanner](#) to find the source of the infection and broken pages respectively.

Your WordPress core files are clean and were not modified.

Audit Report

The data used to generate these charts comes from the last 500 audit logs, you can configure this number from the plugin settings page, you can also disable and enable this panel from there at any time.

Audit Logs per Event

source <https://sucuri.net/>

Event Type	Percentage
Critical Events	52.0%
Warning Events	34.1%
Error Events	8.4%
Info Events	5.6%
Debug Events	0.0%
Notice Events	0.0%

Successful/Failed Logins

source <https://sucuri.net/>

Login Status	Percentage
Failed Logins	61.9%
Successful Logins	38.1%

Audit Logs per User

source <https://sucuri.net/>

User	Count
system	24
[User]	44
[User]	109
[User]	1
[User]	1

Audit Logs per IP Address

source <https://sucuri.net/>

IP Address	Count
42.114.179.81	1
119.81.140.206	4
127.0.0.1	20
42.115.167.147	9
37.115.191.239	2
118.71.78.33	85
201.18.18.173	12
222.252.57.166	4
42.115.185.175	13
42.114.179.67	3
109.230.220.9	1
14.232.28.204	2
118.71.153.66	20
222.252.39.46	3

Audit Logs (50 latest logs)

Date	Username	IP Address	Event Message
14/06/2017 10:49	[User]	42.114.179.81	User authentication succeeded: daoduybinh
09/06/2017 05:34	system	119.81.140.206	Post deleted; identifier: 3
08/06/2017 17:53	system	127.0.0.1	New file added: (multiple entries): <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px; font-family: monospace; font-size: 0.8em;"> .htaccess (size: 861) google17ec1c48eb8c6357 (3).html (size: 53) google17ec1c48eb8c6357.html </div>

Bản quyền ấn phẩm thuộc về <https://wpcanban.com>

Trên đây là toàn bộ những lời khuyên và thủ thuật mà bạn nên áp dụng để đảm bảo an toàn cho blog/ website WordPress của mình. Chúng là những kinh nghiệm được tích lũy nhiều năm liên hoạt động trong lĩnh vực WordPress của tôi. Chắc hẳn sẽ còn rất nhiều thiếu sót. Chúng tôi rất mong nhận được sự đóng góp ý kiến của các bạn để hoàn thiện ebook trong thời gian sắp tới.

Mọi thắc mắc và ý kiến đóng góp xin gửi về email trunghieubui93@gmail.com để được hỗ trợ, giải đáp.

Xin trân trọng cảm ơn!

Tác giả
Bùi Trung Hiếu

[WP Căn bản](#) giữ bản quyền ebook này. Vui lòng không bán hoặc chia sẻ lại nếu không có sự đồng ý của chúng tôi. Xin cảm ơn!