CyStack

Bảo mật website A – Z:

Từ chiến lược đến thực thi

MỤC LỤC

A. THỰC TRẠNG

B. CHIẾN LƯỢC BẢO MẬT WEBSITE TOÀN DIỆN

C. DỊCH VỤ BẢO MẬT WEBSITE TỪ CYSTACK

D. TỔNG KẾT

A. THỰC TRẠNG

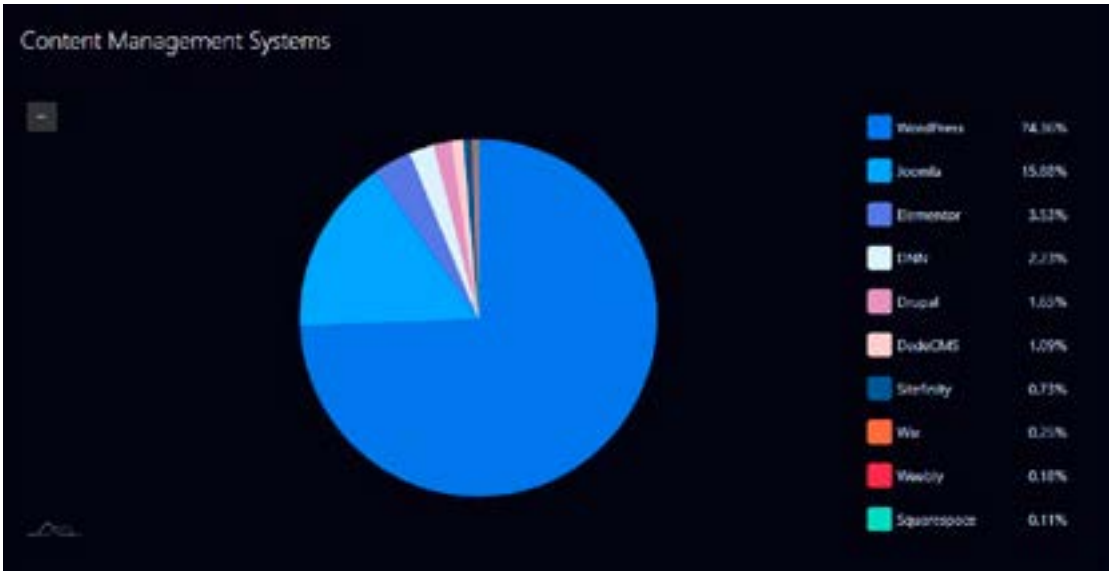
1. TÌNH HÌNH AN NINH WEBSITE 2019

Theo Bản đồ Tấn công website toàn cầu (01/01/19 – 30/06/19), Việt Nam xếp thứ 11 trong số các nước bị hack website nhiều nhất trên thế giới. Trung bình mỗi tháng có tới 1000 website bị xâm phạm – tương đương 35 trang web bị hack mỗi ngày.

Vietnam lọt Top 11 các quốc gia có website bị hack nhiều nhất trên thế giới.
Theo ***CyStack Attack Map***

So với 2018, số vụ tấn công năm 2019 tuy giảm đi, nhưng **quy mô tấn công** lại có chiều hướng gia tăng, thiệt hại cũng lớn hơn so với cùng kỳ năm trước.

WordPress tiếp tục là nền tảng quản trị nội dung (CMS) bị tấn công nhiều nhất – chiếm tới 74.3% tổng số các website bị hack trên toàn cầu. Ngay sau đó là Joomla với 15.9%, Drupal chỉ chiếm 1.65%.



WordPress là nền tảng CMS bị hack nhiều nhất trên thế giới.

Nguồn: ***CyStack Attack Map***

Trên WordPress, hacker dễ dàng **phát tán Mã độc** thông qua các **Theme hay Plugin miễn phí**. Khi người dùng tải về và cài đặt, mã độc được tự động chèn vào website và thực thi những câu lệnh độc hại. Qua đó thực hiện các hành vi xâm phạm, tấn công, chiếm tài nguyên website cũng như máy chủ.

Bên cạnh các hình thức tấn công quen thuộc như *Brute force*, *Phishing*, *D-DoS*, sự gia tăng của *Cross-site Scripting (XSS)*, *SQL injection* tạo nên xu hướng tấn công mới cho năm 2018 và 2019, gây không ít khó khăn cho các chủ website trong việc phòng thủ, bảo vệ trang web của mình.

2. NHỮNG TÁC HẠI KHI TRANG WEB BỊ HACK!

Gián đoạn hoạt động kinh doanh

Rất nhiều doanh nghiệp đang kinh doanh thông qua website. Việc website không thể truy cập chắc chắn sẽ làm mất đi số lượng lớn khách hàng vốn có. Lượng khách hàng này sẽ mất dần vào tay các đối thủ cạnh tranh của bạn.

Ảnh hưởng đến SEO (Từ khóa bị mất thứ hạng trên Google)

Nếu website bị nhiễm mã độc hoặc virus, Google sẽ gỡ trang của bạn trong trang kết quả tìm kiếm (SERP). Việc này ảnh hưởng trực tiếp tới các chiến dịch marketing online của doanh nghiệp.

Ảnh hưởng tới uy tín thương hiệu

Những website liên tục không thể truy cập hoặc bị báo cáo virus sẽ làm giảm lòng tin khách hàng. Thiệt hại về uy tín và thương hiệu kinh doanh của bạn lúc này là rất lớn.

Website bị hack ảnh hưởng tới ***trải nghiệm người dùng*** *và* ***uy tín thương hiệu****.*

Ảnh: internet

Không thể chạy quảng cáo Google và Facebook

Khi website gặp sự cố, bạn không có Destination URL để chạy *Google Ads* cũng như *Facebook Lead/Conversion Ads*. Đây sẽ là thiệt hại lớn cho các công ty ứng dụng digital marketing vào bán hàng.

3. DOANH NGHIỆP VỪA VÀ NHỎ LÀ MỤC TIÊU HẤP DẪN!

Khi tư vấn cho các doanh nghiệp vừa và nhỏ (SMB) tại Việt Nam, tôi gặp hàng tá lý do để bao biện cho sự *thiếu quan tâm tới bảo mật web*. Dưới đây là 3 lý do phổ biến nhất:

- ***"Website của anh chẳng có gì đáng để hack"***
- ***"Hack web của anh để làm gì?"***
- ***"Web của anh không nổi tiếng, làm gì có ai biết mà hack?"***

Nếu bạn cũng đang có suy nghĩ như vậy, thì hãy xem tiếp nhé!

"Website của tôi chẳng có gì để hack"

Câu trả lời: Bạn đang đánh giá thấp website của mình!

Thực tế chứng minh **website là một trong những kênh kinh doanh hiệu quả nhất**: từ chốt đơn – bán hàng, thu thập leads, re-marketing, tới chạy Ads, SEO, chăm sóc khách hàng, tăng nhận diện thương hiệu,...

Chính vì vậy, việc website của bạn bị tấn công có thể gây ra sự *tụt giảm đáng kể trong doanh thu* và *uy tín thương hiệu*. Vấn đề càng trở nên trầm trọng hơn đối với các doanh nghiệp *kinh doanh thông qua trang web* như: thương mại điện tử, ngân hàng, agency du lịch – OTA, ví điện tử, sàn giao dịch, kinh doanh online, bảo hiểm, y tế, tài chính...

"Hack trang web của tôi để làm gì?"

Câu trả lời: Website của bạn mang lại nhiều lợi ích cho hacker hơn bạn tưởng!

Tin tặc có 1001 lý do để hack TẤT CẢ các trang web trên internet. Bạn không nghe lầm đâu, là TẤT CẢ – càng nhiều càng tốt...

Khi hack được một website, chúng có thể:

- Biết được thông tin quan trọng trong cơ sở dữ liệu (thông tin thẻ tín dụng, thông tin khách hàng,...).
- Điều hướng khách hàng tới trang lừa đảo (phishing)
- Lợi dụng tài nguyên (băng thông) của hệ thống để Đào tiền ảo bitcoin, đặt quảng cáo trên trang của bạn.
- Bán website, bán thông tin người dùng
- Sử dụng website như một công cụ để trục lợi trong SEO: tăng uy tín cho web của chúng, kéo traffic, cài cắm backlink bẩn, Redirect 301, v.v...

Trên đây mới chỉ là một vài lợi ích cơ bản mà một website mang lại cho hacker, đủ hiểu khao khát tấn công website của chúng cao đến đâu.

Website của tôi không nổi tiếng, làm gì có ai biết mà hack?"

Câu trả lời: tin tặc chẳng cần biết website của bạn là gì mà vẫn hack được, thế mới tài!

Có một sự thật ít người biết, đó là tin tặc không cần phải biết website của bạn là gì để có thể hack. Thông thường, chúng sử dụng các **công cụ mạnh mẽ** có thể **"quét" tất cả các website trên internet**, từ đó tìm ra các website có bảo mật yếu để tấn công. Bằng chứng là vụ bắt giữ hồi cuối tháng 5/2019 đối với 4 đối tượng "Hacker sinh viên" tại đại học Thái Nguyên – nhóm này đã thực hiện ***quét lỗ hổng của hàng trăm website ngân hàng và trung gian thanh toán*** – sau đó xâm nhập vào các tài khoản và chiếm đoạt số tiền lên tới 3 tỷ đồng.

> *Những website của doanh nghiệp vừa và nhỏ (SMB) dễ bị tấn công hơn so với các công ty lớn. Lý do chính bởi các SMB chưa thực sự quan tâm tới vấn đề bảo mật website của mình.*

Ebook này sẽ giúp bạn xây dựng một chiến lược toàn diện để tăng cường bảo mật cho website lên mức cao nhất. Bắt đầu thôi!

B. CHIẾN LƯỢC BẢO MẬT WEBSITE TOÀN DIỆN

1. CHỐNG TẤN CÔNG PASSWORD

Tấn công password là hình thức tấn công cơ bản nhưng nhiều người vẫn chưa biết cách phòng chống! Trong hình thức này, kẻ tấn công dùng các thủ đoạn và phần mềm độc hại nhằm chiếm mật khẩu của quản trị viên điều hành website.

Dưới đây là các giải pháp đơn giản mà hữu ích giúp bạn bảo vệ mật khẩu của mình:

1.1 Sử dụng mật khẩu mạnh

Phương pháp tấn công Password phổ biến nhất mà hacker sử dụng là Brute-Force Attack. Chúng sẽ sử dụng một công cụ dò mật khẩu tự động để thử tất cả các mật khẩu phổ biến. Vì thế, các quản trị viên được khuyến nghị sử dụng mật khẩu phức tạp để phòng tránh các cuộc tấn công dạng này.

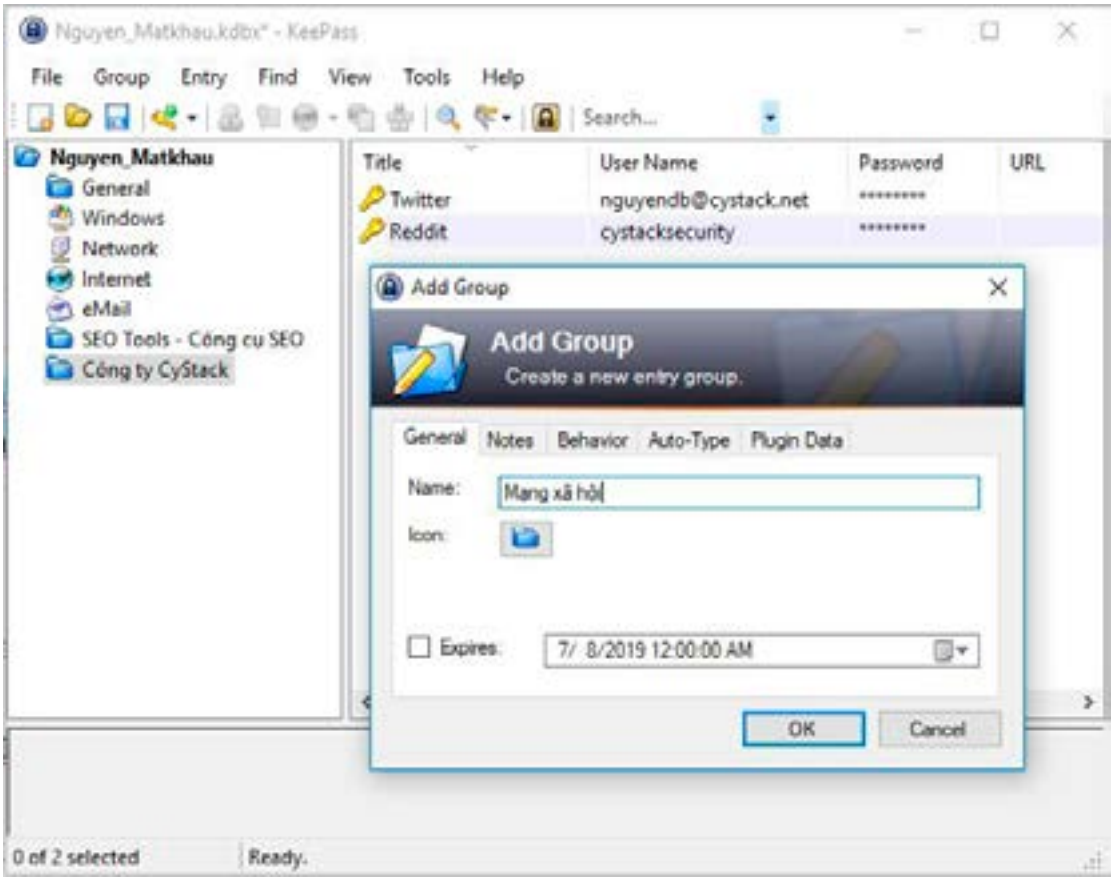
- Mật khẩu nên chứa tất cả các yếu tố: ký tự thường, ký tự in HOA, số, ký tự đặc biệt (!@#$%^&*...). Điều này khiến tin tặc khó tấn công dò tìm mật khẩu hơn. Đặc biệt, nếu mật khẩu của bạn là 1 chuỗi ký tự vô nghĩa thì càng tốt!
- Không đặt mật khẩu trùng nhau cho các dịch vụ khác nhau (VD: password facebook cá nhân phải khác password quản trị web, khác luôn password G-mail). Việc này giúp giảm thiểu thiệt hại khi bạn bị mất mật khẩu.

Mặc dù 2 điều trên rất dễ thực hiện, nhưng hiệu quả lại vô cùng lớn trong việc bảo mật trang web của bạn. Một sự thực đáng buồn là nhiều người còn chưa thực hiện do không nhớ được các mật khẩu đã tạo ra.

Vì vậy, tôi sẽ giới thiệu với các bạn một ứng dụng rất hay để quản lý mật khẩu cá nhân. Đó là Keepass!

> *KeePass là một công cụ mạnh mẽ giúp quản lý tất cả mật khẩu của bạn.*

Sử dụng Keepass rất đơn giản: Bạn tạo một file lưu tất cả mật khẩu các dịch vụ mà bản thân sử dụng, Keepass sẽ giúp bạn mã hóa chúng. Ngoài ra, Keepass hỗ trợ tạo mật khẩu ngẫu nhiên – khó đoán cho người dùng.



Phần mềm cũng hỗ trợ chia nhóm dịch vụ (group) để dễ dàng quản lý.

Bạn có thể sử dụng các mật khẩu bất kỳ lúc nào bằng cách bật Keepass và copy chúng, dán lên trình duyệt.

Việc quan trọng duy nhất bạn cần làm là bảo đảm an toàn cho file dữ liệu này. Tải về Keepass tại trang chủ: ***Keepass.info***

Xem thêm: ***Bị mất mật khẩu phải làm sao?***

1.2 Bật xác thực 2 bước

Một cách hữu hiệu khác để chống lại tấn công mật khẩu ***Bruteforce*** là bật xác thực 2 bước cho trình quản lý. Bởi ngay cả khi kẻ tấn công đoán đúng mật khẩu, chúng cũng không thể đăng nhập nếu như bạn bật xác thực 2 bước (two-factor authentication).

Các nền tảng quản lý nội dung hiện nay đều hỗ trợ tính năng này thông qua hệ thống Plugin (WordPress) hay Extension (Joomla).

Bật xác thực 2 bước cho WordPress

Có nhiều plugin trên WordPress giúp bạn xác minh 2 bước khi đăng nhập, nhưng tôi chỉ sử dụng Google Authenticator (miễn phí) bởi tính tiện dụng của nó. Bạn chỉ cần cài đặt Plug-in Google Authenticator từ kho plugin của WordPress. Sau khi cài đặt thành công, hãy bật tính năng này lên và quét mã QR bằng ứng dụng ***Google Authenticator*** trên smartphone của bạn (hỗ trợ Android, iOS, Blackberry). DONE!

Để đăng nhập những lần tiếp theo, bạn chỉ việc nhập username & password, sau đó nhập mã từ ứng dụng Google Authenticator là xong.

Lưu ý: Hiện tại vẫn chưa hỗ trợ cài đặt 1 lần cho nhiều tài khoản. Vì thế, bạn phải cài 2FA thủ công cho từng tài khoản quản trị viên.

1.3 Giới hạn đăng nhập

Bạn có thể phòng chống tấn công dò mật khẩu bằng cách giới hạn số lần nhập sai password.

iThemes là một trong những plugin WordPress tốt nhất để thực hiện điều này. Plugin này cho phép chặn nỗ lực đăng nhập trái phép và ngay lập tức thông báo cho chủ website thông qua email. Bất cứ khi nào có một nỗ lực tấn công với các mật khẩu sai liên tục lặp đi lặp lại, website sẽ bị khóa, và bạn sẽ nhận được thông báo về hoạt động trái phép này.

Bạn hoàn toàn có thể set up chế độ bảo mật riêng, tự hạn chế số lần người dùng đăng nhập vào hệ thống. Ví dụ như chỉ cho phép người dùng đăng nhập tối đa 5 lần, quá ngưỡng này thì cấm địa chỉ IP đó.

>> Tải về iThemes Security cho WordPress

Sau khi cài đặt, bạn sẽ nhận được một thông báo yêu cầu kích hoạt tính năng **iThemes Brute Force Network Protection** (miễn phí). Chương trình này kết nối trang web của bạn với iThemes Network, như vậy các hacker sử dụng phương thức brute force để tấn công website sẽ ngay lập tức bị chặn và khóa vĩnh viễn.

Quá trình cài đặt khá đơn giản, bạn chỉ cần điền địa chỉ email để nhận mã API miễn phí. Sau đó, truy cập vào **Security » Settings** để chọn và tùy chỉnh các cài đặt bảo mật phù hợp với website của mình.

1.4 Đổi URL đăng nhập trang quản lý

Thông thường, để đăng nhập vào trình quản lý của website, bạn thường truy cập vào 1 trong những địa chỉ sau:

- ten_mien.com/wp-admin (wordpress)
- ten_mien.com/wp-login.php
- ten_mien.com/administrator/index.php (joomla)

Vì đây là những đường dẫn (URL) đăng nhập mặc định, nên tin tặc có thể dễ dàng đoán được, từ đó mở đầu một cuộc tấn công Password. Để thay đổi đường dẫn này, trong WordPress bạn dùng plugin iTheme Security. Nếu bạn sử dụng Joomla, hãy tải và cài đặt tiện ích mở rộng (extension) có tên "Change Administrator".

>> Tải về iTheme Security cho WordPress

>> Tải về Change Administrator cho Joomla

2. PHÒNG CHỐNG MÃ ĐỘC

> *Mã độc là một kênh tấn công website "xưa như trái đất", nhưng chưa bao giờ "lỗi thời"!*

Thế giới công nghệ càng phát triển, tin tặc càng nghĩ ra nhiều mã độc (malware) phức tạp, nguy hiểm hơn, gây thiệt hại nghiêm trọng hơn cho nạn nhân. Một số mã độc mà website thường nhiễm phải: virus, trojan, adware, spyware, coinhive...

Xem thêm tại infographic: ***Muôn hình vạn trạng các loại Malware***

- Mã độc gây gián đoạn, cản trở hoạt động của website
- Hiện quảng cáo thu lợi cho kẻ tấn công
- Tận dụng tài nguyên hệ thống để đào Bitcoin
- Chuyển hướng người dùng sang trang lừa đảo và nhiều tai hại khác.

Dưới đây là một số gợi ý giúp website an toàn khỏi các phần mềm độc hại:

2.1 Quét mã độc Website thường xuyên

Cũng giống như bạn quét virus cho máy tính, website cũng cần được "làm sạch" khỏi sự xâm lăng của mã độc. Việc làm này giống như một thủ tục định kỳ và có thể gây nhàm chán. Nhưng...

Thà nhàm chán còn hơn để website bị nhiễm mã độc, phải không nào!

Hơn nữa, hiện nay hầu hết các phần mềm quét mã độc cho website đều có tính năng Đặt lịch quét (Schedule Scan) giúp cho việc bảo mật web dễ dàng hơn.

>> Hướng dẫn quét mã độc cho Website

2.2 Luôn cập nhật phiên bản mới

Những bản cập nhật của website có lúc gây cảm giác phiền toái, nhưng đôi khi chúng là "phao cứu sinh" giúp bạn tránh khỏi những cuộc tấn công mạng nguy hiểm.

Mặc dù WordPress là CMS bị hack nhiều nhất trên thế giới, tuy nhiên hệ quả này không hẳn tới từ việc WordPress bảo mật kém. Bản thân đội ngũ phát triển WordPress luôn làm việc để tung ra các bản vá bảo mật, và cung cấp cho người dùng dưới dạng các bản cập nhật WordPress. Vì thế nếu bạn sử dụng Joomla hay WordPress, hãy luôn đảm bảo cập nhật các phiên bản mới nhất cho website của mình để đề phòng rủi ro.

2.3 Nói KHÔNG với Theme và Plugin không rõ nguồn gốc!

> *Theme và Plugin không rõ nguồn gốc là mối "đại họa" cho website của bạn!*

Rất nhiều tin tặc lợi dụng tâm lý "ham rẻ" của các webmaster để tấn công website thông qua việc tạo ra những Themes/Plugins miễn phí có chứa Mã độc!

Sau khi người dùng tải về và cài đặt lên trang web của mình, mã độc trong Theme/plugin bắt đầu thực hiện những hành vi gây hại, *làm gián đoạn website và để lại nhiều hệ lụy khác.*

Điều này có đồng nghĩa với việc: **"Không được sử dụng Theme và Plugin miễn phí???"**

Câu trả lời là KHÔNG! Bạn vẫn có thể sử dụng Theme và Plugin miễn phí. Tuy nhiên, phải kiểm tra nguồn gốc xuất sứ của chúng. Hãy đảm bảo rằng các theme/plugin miễn phí bạn sử dụng được phát hành bởi một đơn vị có uy tín và đáng tin cậy.

Trên thực tế, có rất nhiều plugin WordPress miễn phí rất hữu ích cho các webmaster mà bạn có thể sử dụng.

3. GIẢM THIỂU TẤN CÔNG DDOS

Có một sự thật mà chúng ta phải công nhận với nhau: Không có giải pháp chống lại HOÀN TOÀN **tấn công DDoS**, chỉ có thể giảm thiểu khả năng bị tấn công VÀ giảm thiểu thiệt hại. Website càng tạo ra nhiều giá trị thì khi bị DDoS càng ảnh hưởng nghiêm trọng tới doanh thu. Dưới đây là một vài thủ thuật cơ bản để **hạn chế bị tấn công DDoS**:

3.1 Phân tích traffic website

Hầu hết các cuộc tấn công DDoS đều bắt đầu bằng sự gia tăng đột biến về lưu lượng truy cập. Do đó, một trong những cách ngăn chặn sớm các cuộc tấn công DDOS là nghiên cứu hồ sơ lưu lượng truy cập (traffic) website của mình. Khi bạn càng hiểu rõ về traffic thông thường của website, bạn càng dễ phát hiện nguy cơ ngay khi có sự thay đổi.

Ví dụ: Website của bạn được thiết kế cho thị trường Việt Nam, bỗng dưng traffic từ Singapore tăng đột biến. Đó có thể là dấu hiệu của một cuộc tấn công DDOS.

3.2 Sử dụng Tường lửa ứng dụng Web

Tường lửa Website (Web Appication Firewall – WAF) là một lớp phòng thủ hữu hiệu, giúp máy chủ web tránh khỏi những hình thức tấn công phổ biến như XSS, SQL injection, Buffer Overflow, hay DDOS. Nhiệm vụ của Tường lửa Website là "sàng lọc" và phân loại các luồng traffic vào website. Từ đó phát hiện và ngăn chặn các luồng traffic được cho là độc hại.

CyStack WebShield là một ứng dụng bảo mật website mạnh mẽ & hoàn toàn tự động. Được tích hợp các tính năng **Tường lửa thông minh** lọc traffic độc hại, Chống tấn công Brute-Force, Quét mã độc, Quét bảo mật tổng thể cho website cùng nhiều tính năng hữu ích khác.

>> Khám phá tính năng WebShield

3.3 Băng thông dự phòng

Bạn nên sử dụng băng thông rộng hơn mức bạn cần cho máy chủ web. Bằng cách đó, bạn có thể đáp ứng các đột biến bất ngờ trong lưu lượng truy cập – có thể là kết quả của một chiến dịch quảng cáo, một chương trình khuyến mãi đặc biệt mà công ty bạn đang sử dụng hay do tên công ty của bạn được đề cập trên các phương tiện truyền thông.

Thực tế, dù bạn có sử dụng băng thông rộng gấp 100% hay thậm chí 500% so với nhu cầu thực tế cũng không chắc chắn sẽ ngăn chặn được một cuộc tấn công DDoS nhưng nó có thể cho bạn thêm vài phút để hành động trước khi máy chủ bị quá tải.

3.4 Giám sát website 24/7

Nếu DDoS là là vấn đề của bạn. Chắc chắn bạn sẽ cần một phần mềm Giám sát Website (Uptime/Downtime) hiệu quả.

Downtime là khoảng thời gian website không khả dụng với người truy cập. Downtime xảy ra có thể do web bị tấn công từ chối dịch vụ (DDoS), có thể website bị quá tải, hoặc có vấn đề xảy ra với dịch vụ Hosting mà bạn đang sử dụng. Một website cần tối đa uptime và giảm thiểu downtime

Trên thị trường hiện có rất nhiều phần mềm Giám sát Website tốt, cả miễn phí và trả phí. Phần mềm miễn phí tốt nhất trên thị trường hiện tại là Uptime Robot. Nó giúp bạn giám sát website theo chu kỳ 5 phút 1 lần, với giao diện thân thiện, dễ sử dụng.

>> Link *Đăng ký sử dụng Uptime Robot* (miễn phí)

4. BẢO VỆ DỮ LIỆU WEBSITE VÀ THÔNG TIN KHÁCH HÀNG

4.1 Cài đặt HTTPS – chứng chỉ SSL

> *Hiện tại đã là năm 2019, bất cứ Website nào cũng nên sử dụng HTTPS!*

Phần mềm cũng hỗ trợ chia nhóm dịch vụ (group) để dễ dàng quản lý.

Tại sao ư?

- **HTTPS bảo mật hơn:** chứng chỉ SSL giúp mã hóa thông tin người dùng gửi tới server (bao gồm tài khoản, mật khẩu, thẻ tín dụng, thông tin cá nhân...) và ngược lại. Từ đó bảo vệ thông tin của người dùng và Server web khỏi Tin tặc.
- **HTTPS tốt cho thương hiệu:** sở hữu *khóa xanh bảo mật* làm cho website của bạn nhìn chuyên nghiệp và đáng tin cậy hơn.
- **HTTPS tốt cho SEO:** Google ưu tiên xếp hạng cao hơn cho những trang web sử dụng HTTPS trên *trang kết quả tìm kiếm* (SERP).
- **Google thích HTTPS!** Đúng vậy. Và không chỉ Google, mà các trình duyệt khác như Firefox, Safari... đều khuyến khích các website sử dụng HTTPS.
- Quan trọng hơn hết, nó **MIỄN PHÍ**!

Thông tin mà người dùng gửi tới Server được mã hóa.

Trước đây, để có được tích xanh bảo mật cho trang web, bạn phải trả một khoản phí cho bên thứ 3 chịu trách nhiệm xác thực "website chính chủ" (Comodo, Symantec, GeoTrust...). Vì thế, chỉ những trang web ngân hàng, TMĐT, tài chính, ví điện tử... mới phải đầu tư cho khoản phí này. Nhưng ở thời điểm hiện tại, **HTTPS đã MIỄN PHÍ cho tất cả trang web!**

>> Hướng dẫn Cài đặt chứng chỉ SSL (HTTPS) miễn phí

4.2 Hạn chế cho phép upload file

> *Việc cho phép người dùng tải file lên trang web có thể mang lại rủi ro lớn cho website của bạn, NGAY CẢ KHI đó chỉ là hành động thay đổi hình đại diện.*

Những file được upload lên, dù trông có vẻ vô hại, thì cũng có thể chứa những dòng lệnh độc hại tiêm nhiễm vào máy chủ. Vì thế, bạn nên "thẳng tay" tắt tính năng upload file nếu không cần thiết.

Nếu bạn bắt buộc phải cho người dùng upload file, hãy cẩn trọng với mọi tình huống. Đặc biệt, bạn không thể chỉ dựa vào phần mở rộng để xác định đó là file hình ảnh. Bởi một file có tên image.jpg.php có thể vượt qua dễ dàng. Ngoài ra thì hầu hết các hình ảnh đều cho phép lưu trữ một phần bình luận (comment) có thể chứa code PHP được thực thi bởi máy chủ web.

Giải pháp cho vấn đề này là chặn hoàn toàn quyền truy cập trực tiếp vào các file được tải lên. Theo đó, mọi file tải lên website được lưu trữ trong một thư mục bên ngoài webroot hoặc trong cơ sở dữ liệu dưới dạng blob. Nếu các file không thể truy cập trực tiếp, sẽ cần tạo một tập lệnh để tìm nạp các file từ thư mục riêng (hoặc trình xử lý HTTP trong .NET) và gửi chúng đến trình duyệt. Thẻ img hỗ trợ thuộc tính src không phải là URL trực tiếp đến hình ảnh, vì vậy thuộc tính src có thể trỏ đến tập lệnh phân phối file, cung cấp loại nội dung chính xác trong tiêu đề HTTP.

4.3 Xác thực từ 2 phía

Xác thực phải luôn luôn được thực hiện cả trên trình duyệt và phía máy chủ. Trình duyệt có thể gặp các lỗi đơn giản như khi các trường bắt buộc điền bị để trống hay nhập văn bản vào trường chỉ cho điền số. Tuy nhiên, những điều này có thể được bỏ qua và nên đảm bảo việc kiểm tra các xác thực sâu hơn phía máy chủ. Vì không làm như vậy có thể dẫn đến mã hoặc tập lệnh độc hại được chèn vào cơ sở dữ liệu hoặc có thể gây ra kết quả không mong muốn trong trang web.

4.4 Cẩn thận với các thông báo lỗi

Hãy cẩn thận với lượng thông tin bạn cung cấp trong các thông báo lỗi. Chỉ cung cấp các lỗi tối thiểu cho người dùng, để đảm bảo chúng không làm rò rỉ các bí mật có trên máy chủ (ví dụ, khóa API hoặc mật khẩu cơ sở dữ liệu). Đừng cung cấp đầy đủ chi tiết ngoại lệ vì những điều này có thể làm cho các cuộc tấn công phức tạp như SQL injection được thực hiện dễ dàng hơn nhiều. Giữ các lỗi chi tiết trong nhật ký máy chủ và chỉ hiển thị cho người dùng thông tin họ cần.

4.5 Sao lưu website định kỳ

> *Sao lưu dữ liệu web (hay backup website) là một công đoạn tối quan trọng trong việc quản trị, bảo mật và phát triển web.*

Việc sao lưu web thường xuyên giúp cho các webmaster chủ động ứng phó trong trường hợp trang web bị hack hay gặp sự cố. Có 2 hình thức sao lưu chính: offline và online.

Với hình thức sao lưu web offline, các chủ web sẽ tải toàn bộ dữ liệu cần thiết của website về máy tính hoặc ổ cứng. Như vậy, bản sao lưu có an toàn hay không nằm ở việc bạn bảo vệ ổ cứng máy tính như thế nào. Tuy nhiên hiện tại, nhờ sự phát triển của công nghệ điện toán đám mây (cloud computing), bạn có thể **sao lưu dữ liệu trên mây** với **giá cả phù hợp, lại bảo mật và tiện lợi hơn** nhiều so với offline backup. Theo đó, toàn bộ dữu liệu cần thiết sẽ được tải lên không gian lưu trữ đám mây. Khi cần thiết, chủ web có thể truy xuất dữ liệu tùy ý, từ bất kì đâu, chỉ cần có internet.

Mấu chốt của việc lưu trữ trên nền tảng đám mây là chọn đối tác uy tín, do việc bảo mật hoàn toàn phụ thuộc vào bên cung cấp dịch vụ. Chúng tôi khuyên chọn những nhà cung cấp uy tín như Amazon với **AWS** hay Microsoft với ***Microsoft Azure***.

5. CHỐNG TẤN CÔNG KHAI THÁC LỖ HỔNG

Lỗ hổng bảo mật của website (web vulnerability) là những điểm yếu của hệ thống website có thể bị kẻ xấu lợi dụng và khai thác, qua đó tấn công website. Những điểm yếu này có thể xuất phát từ mã nguồn (source code) của web, lỗi của lập trình viên, hoặc do website phức tạp (càng nhiều tính năng thì càng dễ xuất hiện nhiều điểm yếu).

Tham khảo: ***Lỗ hổng website là gì và 10 lỗ hổng phổ biến nhất***

Phần lớn những lỗ hổng này có thể được phát hiện bằng phần mềm chuyên dụng. Một số lỗ hổng phức tạp hơn đòi hỏi thực hiện phương pháp Pentest (kiểm thử bảo mật) sẽ được đề cập trong **phần số 8.**

Trong phần này, tôi sẽ giới thiệu 2 lỗ hổng phổ biến là "xu hướng tấn công" năm 2019 và các công cụ tự động để quét lỗ hổng bảo mật hiệu quả.

5.1 Lỗ hổng SQL injection

Các cuộc tấn công **SQL injection** là khi kẻ tấn công sử dụng trường mẫu web hoặc tham số URL để có quyền truy cập hoặc thao tác cơ sở dữ liệu của nạn nhân. Khi sử dụng Transact SQL tiêu chuẩn, thật dễ dàng chèn code giả mạo vào truy vấn của người dùng, từ đó thay đổi bảng, lấy thông tin và xóa dữ liệu. Có thể dễ dàng ngăn chặn điều này bằng cách luôn sử dụng truy vấn được tham số hóa. Hầu hết các ngôn ngữ web đều có tính năng này và nó rất dễ thực hiện.

Xem xét truy vấn sau:

```
"SELECT * FROM table WHERE column = '" + parameter + "';"
```

Nếu kẻ tấn công thay đổi tham số URL thành ‘ or ‘1’=’1 thì điều đó sẽ khiến truy vấn trông như sau:

```
“SELECT * FROM table WHERE column = ‘’ OR ‘1’=’1’;”
```

Vì ‘1’ bằng ‘1’, điều này sẽ cho phép kẻ tấn công thêm một truy vấn bổ sung vào cuối câu lệnh SQL và nó cũng sẽ được thực thi.

Bạn có thể sửa truy vấn này bằng cách tham số hóa nó một cách rõ ràng. Ví dụ, nếu đang sử dụng MySQLi trong PHP thì truy vấn sẽ trở thành:

```
$stmt = $pdo->prepare(‘SELECT * FROM table WHERE column = :value’);

$stmt->execute(array(‘value’ => $parameter));
```

5.2 Lỗ hổng XSS (Cross-site Scripting)

Cross-site scripting (XSS) truyền JavaScript độc hại vào các trang web, sau đó chạy trong trình duyệt của người dùng và có thể thay đổi nội dung trang, hoặc đánh cắp thông tin để gửi lại cho kẻ tấn công.

Đây là mối quan tâm đặc biệt trong các ứng dụng web hiện đại, nơi các trang hiện được xây dựng chủ yếu từ nội dung người dùng và tạo HTML cũng được biên dịch bởi các framework front-end như Angular và Ember trong nhiều trường hợp. Các framework này cung cấp nhiều biện pháp bảo vệ chống lại XSS, nhưng việc kết hợp rendering máy chủ và máy khách cũng tạo ra các cách tấn công mới và phức tạp hơn, không chỉ có khả năng truyền JavaScript vào HTML hiệu quả, mà còn có thể truyền nội dung sẽ chạy code bằng cách chèn các lệnh Angular hoặc sử dụng các trình trợ giúp Ember.

Mấu chốt ở đây là tập trung vào cách nội dung do người dùng tạo. Điều này tương tự như bảo vệ chống lại SQL injection. Khi tạo HTML động, hãy sử dụng các hàm thực hiện rõ ràng các thay đổi đang tìm kiếm (ví dụ, sử dụng phần tử **.setAttribution** và **Element.textContent** để trình duyệt tự động escape, thay vì cài đặt phần tử.innerHTML thủ công) hoặc sử dụng các hàm tự động escape khi thích hợp, thay vì nối chuỗi hoặc đặt nội dung HTML thô.

Một công cụ mạnh mẽ khác để chống lại XSS là chính sách bảo mật nội dung (Content Security Policy – CSP). CSP là header máy chủ có thể trả về, cho phép trình duyệt giới hạn cách thức và những gì JavaScript được thực thi trong trang, ví dụ như không cho phép chạy bất kỳ tập lệnh nào không được lưu trữ trên domain, không cho phép JavaScript nội tuyến hoặc vô hiệu hóa **eval()**. Mozilla có một hướng dẫn tuyệt vời với một số cấu hình ví dụ (tham khảo tại developer.mozilla.org/en-US/docs/Web/HTTP/CSP). Điều này làm cho các tập lệnh của kẻ tấn công khó hoạt động hơn, ngay cả khi kẻ tấn công có thể đưa chúng vào trang web.

5.3 Phần mềm chuyên dụng quét lỗ hổng tự động

Mặc dù trên thị trường có rất nhiều phần mềm quét lỗ hổng website, nhưng không phải phần mềm nào cũng được việc. Dưới đây là một trong những phần mềm quét lỗ hổng phổ được tin dùng nhất:

- **IBM Security AppScan Standard**
- **Tenable**
- **Arachni**
- **CyStack WebShield**

Ưu – nhược điểm, giá cả, tính năng của mỗi phần mềm sẽ được phân tích kỹ trong link bên dưới. Các bạn tham khảo thêm.

Đánh giá chi tiết: ***Top 10 ứng dụng scan lỗ hổng website tốt nhất trên thị trường***

WebShield là một ứng dụng SaaS (cloud-based) hỗ trợ **quét lỗ hổng bảo mật web** hiệu quả mà không cần cài đặt. Ngoài ra, WebShield được tích hợp tính năng **quét mã độc**, **quét bảo mật tổng thể** cho website và nhiều tính năng hữu ích khác. Mức giá được thiết kế phù hợp với doanh nghiệp vừa và nhỏ.

>> Khám phá tính năng WebShield

6. BẢO MẬT HOSTING VÀ CƠ SỞ DỮ LIỆU WEB

Hãy chọn một dịch vụ Hosting UY TÍN thay vì GIÁ RẺ !!

Một đối tác Hosting uy tín sẽ có trách nhiệm với những "biến cố" xảy ra với website của bạn. Hiện nay trên thị trường, nhiều nhà cung cấp hosting giá rẻ có tình trạng "đem con bỏ chợ". Lúc mời gọi mua dịch vụ thì rất nhiệt tình, còn lúc khách cần thì không thấy đâu. Bạn nên tham khảo kỹ trước khi lựa chọn dịch vụ hosting, vì không những ảnh hưởng tới bảo mật, xử lý sự cố, mà hosting còn ảnh hưởng tới SEO nữa đấy!

6.2 Giữ cho website sạch sẽ

Website càng nhiều tính năng thì nguy cơ xuất hiện những điểm yếu cho tin tặc khai thác càng cao. Vì vậy, việc cần làm là tắt tất cả những tính năng (bao gồm plugin trong wordpress, extension trong Joomla,...) không sử dụng đến hoặc không quá quan trọng. Quản trị viên website cần hiểu rõ về công việc kinh doanh của mình, mục đích sử dụng của website, từ đó tạo ra một hệ thống web đủ dùng, tối giản mà vẫn hiệu quả.

6.3 Bật xác thực 2 bước đăng nhập Hosting

Để bảo mật hosting tốt hơn, bạn nên thiết lập xác minh 2 bước khi đăng nhập vào trình quản lý Hosting. Cụ thể trong bài viết này, tôi sẽ hướng dẫn bạn thực hiện với cPanel HawkHost, các dịch vụ hosting khác bạn có thể làm tương tự. Quy trình thực hiện như sau:

- Tải và cài đặt một ứng dụng 2FA bất kì về smartphone. *Các ứng dụng phổ biến: Google Authenticator (Hỗ trợ Android, iOS, blackberry), Duo Mobile (Hỗ trợ Android, iOS), Authy (hỗ trợ Android, iOS, Blackberry).*
- Đăng nhập vào giao diện cPanel, gõ vào thanh tìm kiếm “Two-Factor Authentication”

  Click vào **Cài Đặt**. Chương trình sẽ trả về 1 QR code và 1 mã xác nhận. Dùng smartphone quét QR code. Nếu phần mềm không hỗ trợ quét QR, bạn cần nhập mã xác nhận gồm 6 số >> HOÀN THÀNH!

Lưu ý: Nếu bị mất tài khoản, bạn cần submit ticket cho HawkHost hoặc nhà cung cấp dịch vụ Hosting để lấy lại.

7. NHỮNG HẠNG MỤC KHÁC CẦN THỰC HIỆN

7.1 Phân quyền tài khoản trang quản trị

Nếu bạn có thói quen cấp đầy đủ quyền admin cho mọi quản trị viên thì có lẽ bạn nên suy nghĩ lại. Bởi đó là một trong những thói quen rất xấu khi quản trị web: chỉ cần một tài khoản bị hack, bạn có thể mất kiểm soát hoàn toàn.

Mỗi nhiệm vụ khác nhau nên được phân quyền khác nhau. *Ví dụ: người viết bài sẽ được cấp tài khoản Editor, chỉ có chức năng quản trị nội dung, bài viết.* Việc này giúp tránh được nhiều rủi ro tai hại từ cả bên trong và bên ngoài. Và cũng **đừng quên xóa tài khoản admin khi nhân sự nghỉ việc!**

Với tài khoản khách, người dùng web: thông thường tài khoản khách chỉ cần tính năng cơ bản như gửi và nhận dữ liệu từ máy chủ. Điều này thay đổi tùy vào mục đích website của bạn, nhưng quy tắc bất di bất dịch là: **không bao giờ trao "thừa" quyền hạn cho bất kì một tài khoản nào.**

7.2 Phân chia môi trường test và thực tế

Một lưu ý nhỏ nhưng không thừa: luôn phân chia môi trường test tách biệt hẳn trang web của bạn. Đừng bao giờ test tính năng/cập nhật ngay trên website nếu như bạn không muốn gây trục trặc cho website của mình. Điều này cũng thể hiện thái độ và phong cách làm việc chuyên nghiệp.

7.3 Bảo mật máy tính & sử dụng internet an toàn

Nếu máy tính của bạn bị nhiễm mã độc, đó cũng có thể là rủi ro với website của bạn. Vì thế, hãy bảo mật cho máy tính cá nhân của mình bằng cách sử dụng một phần mềm diệt Virus.

Bên cạnh đó, tập thói quen sử dụng internet an toàn là điều bắt buộc. Một vài lưu ý:

- Không tải file không rõ nguồn gốc
- Không click vào link lạ
- Không click vào quảng cáo ở những trang web đen
- Kiểm tra địa chỉ người gửi mail
- Kiểm tra nội dung email
- ...

7.4 Nâng cao nhận thức cho nhân viên

> *Con người là mắt xích yếu nhất trong đảm bảo an ninh mạng cho tổ chức!*

Đó là nhận xét của ông Nguyễn Hữu Trung – CTO tại CyStack. Thật vậy, có đến 83% các cuộc tấn công website xảy ra xuất phát từ sai lầm của con người (lập trình viên, quản trị web, người dùng web). Vì thế, việc tổ chức các khóa đào tạo – training cho nhân viên về vấn đề bảo mật website, sử dụng internet an toàn là rất cần thiết. Việc đó giúp doanh nghiệp tiết kiệm một khoản lớn chi phí dành cho bảo mật và ứng biến sự cố.

8. PENTEST – KIỂM THỬ WEBSITE

> *Một trong những phương pháp hiệu quả và mạnh mẽ nhất để bảo mật ứng dụng web là Pentest!*

Pentest, hay kiểm thử xâm nhập, là hình thức tăng cường bảo mật bằng cách xâm nhập vào website. Với phương pháp này, các chuyên gia bảo mật sẽ cố gắng tìm mọi cách để xâm nhập vào web của bạn, từ đó tìm ra điểm yếu (lỗ hổng bảo mật) của trang web. Khi đó, bạn có thể dễ dàng khắc phục những điểm yếu này và tăng cường bảo mật cho trang web của mình.

Khi quyết định thuê một dịch vụ Pentest, nên chú ý:

- Chọn các đơn vị có uy tín, kinh nghiệm
- Tìm hiểu rõ các điều khoản bảo mật, cũng như hợp đồng thực hiện
- Chọn phương án phù hợp với tình hình tài chính và giai đoạn phát triển của doanh nghiệp.

Xem ngay: ***Dịch vụ pentest toàn diện, tư vấn miễn phí từ chuyên gia***

9. SỬ DỤNG PHƯƠNG PHÁP BẢO MẬT CỘNG ĐỒNG ĐỂ TĂNG CƯỜNG BẢO MẬT ỨNG DỤNG WEB

9.1 Bảo Mật Cộng Đồng là gì?

Bảo Mật Cộng Đồng (Crowdsourced Security) là phương pháp tận dụng sức mạnh của hacker mũ trắng và các nhà nghiên cứu bảo mật tự do để bảo mật cho website. Về cơ bản, BMCĐ chính là Pentest, nhưng với quy mô rộng hơn. Thay vì 1 nhóm người thực hiện pentest, thì cả cộng đồng chuyên gia sẽ pentest cho website của bạn.

Tải MIỄN PHÍ ebook: ***Crowdsourced Security là gì?***

Phương pháp này được ứng dụng rộng rãi ở Mỹ & châu Âu vì tính thực tiễn của nó. Các doanh nghiệp sẽ không phải "đốt tiền" một cách vô tội vạ, mà họ sẽ chỉ phải tốn một khoản phí làm tiền thưởng cho hacker mũ trắng hoặc chuyên gia bảo mật.

Những tập đoàn lớn đều áp dụng phương pháp này: Google, Facebook, HP, hay cả Bộ Quốc Phòng Mỹ cũng đã khởi chạy chương trình Bug Bounty để bảo vệ hệ thống mạng lưới an ninh.

9.2 Chương trình Bug Bounty

Chương trình Bug Bounty (Trao thưởng tìm lỗi) là cách giúp các doanh nghiệp triển khai Bảo Mật Cộng Đồng. Để bắt đầu, bạn sẽ triển khai một chương trình Bug Bounty: Thưởng tiền mặt cho bất kỳ ai tìm ra lỗ hổng trên website của mình.

Mấu chốt để tạo ra một chương trình Bug Bounty thành công là bạn phải tiếp cận được với một cộng đồng **nhiều chuyên gia bảo mật**. Họ sẽ giúp bạn làm phần việc còn lại (bảo mật trang web của bạn).

Xem ngay: ***Làm sao để tổ chức chương trình Bug Bounty?***

9.3 Các đối tác uy tín

Dưới đây là các đơn vị uy tín cung cấp nền tảng Bug Bounty được ưa chuộng:

- **Bugcrowd** (San Francisco, California)
- **hackerone** (San Francisco | London | New York | Singapore | Hà Lan)
- **Synack** (Redwood City, California)
- **Detectify** (Stockholm, Thụy Điển)
- **Cobalt** (San Francisco | Berlin)
- **AntiHack** (Singapore)
- **WhiteHub** (Việt Nam)
- **Bugbounty.vn** (Việt Nam)

9.4 WhiteHub – Kết nối doanh nghiệp với cộng đồng 500+ chuyên gia bảo mật

WhiteHub là nền tảng Crowdsourced Security **đầu tiên tại Việt Nam**, giúp kết nối nhu cầu kiểm thử bảo mật của doanh nghiệp và cộng đồng chuyên gia tại khắp nơi trên thế giới.

Thông qua WhiteHub, doanh nghiệp có thể **khởi tạo và quản lý chương trình** Bug Bounty, tiếp cận với cộng đồng hơn 500+ chuyên gia bảo mật. Từ đó bảo mật tối đa cho các sản phẩm ứng dụng của mình.

>> Tìm hiểu giải pháp của WhiteHub

9.5 Case study: bảo mật cho website vntrip.vn

Tại Việt Nam, Vntrip là doanh nghiệp nổi bật thực hiện thành công chương trình Bug Bounty, qua đó khắc phục được rủi ro bị hack thông tin của 500,000 khách hàng, và giúp bảo vệ website an toàn, ổn định hơn.

Xem ngay Case study: ***Vntrip đã bảo mật dữ liệu 500.000 khách hàng như thế nào?***

C. DỊCH VỤ BẢO MẬT WEBSITE TỪ CYSTACK

1. QUY TRÌNH HỢP TÁC

1. Đánh giá website

CyStack thực hiện đánh giá tổng thể hệ thống website của doanh nghiệp, bao gồm các hạng mục: Số lượng Domain, mô hình kinh doanh, từ đó phát hiện ra các rủi ro đặc biệt mà doanh nghiệp của bạn đang gặp phải.

2. Đề xuất giải pháp

Mỗi doanh nghiệp đều có những điểm yếu khác nhau. CyStack đề xuất giải pháp được thiết kế riêng cho doanh nghiệp của bạn bao gồm các hạng mục: Công cụ, con người, hạ tầng triển khai.

3. DEMO sản phẩm

Giúp doanh nghiệp lựa chọn sản phẩm và gói cước phù hợp nhất với quy mô hiện tại, từ đó tối ưu chi phí.

4. Hợp tác

Hai bên ký hợp đồng hợp tác. Doanh nghiệp được hỗ trợ trong suốt thời gian triển khai.

2. SẢN PHẨM

2.1 CyStack WebShield

CyStack WebShield là ứng dụng bảo mật web mạnh mẽ & hoàn toàn tự động. Ứng dụng tích hợp các tính năng:

- Quét bảo mật tổng thể cho website
- Tường lửa thông minh giúp lọc các traffic nguy hại cho máy chủ web
- Chống tấn công Brute-Force
- Công cụ dò tìm và tiêu diệt mã độc, làm sạch website
- Quét lỗ hổng web theo OWASP Top 10 & hỗ trợ khắc phục
- Tính năng đặt lịch quét tự động
- Giám sát Uptime website 24/7
- Giám sát & cảnh báo DNS Blacklist
- Phát hiện thay đổi nội dung
- Cảnh báo thông minh qua smartphone, email, PC
- Hỗ trợ HTTPS/SSL miễn phí

>> Xem bảng giá WebShield

2.2 CyStack WhiteHub

WhiteHub là nền tảng Crowdsourced Security **đầu tiên tại Việt Nam**, giúp kết nối nhu cầu kiểm thử bảo mật của doanh nghiệp và cộng đồng chuyên gia tại khắp nơi trên thế giới.

Thông qua WhiteHub, doanh nghiệp có thể **khởi tạo và quản lý chương trình** Bug Bounty, tiếp cận với cộng đồng hơn 500+ chuyên gia bảo mật. Từ đó bảo mật tối đa cho các sản phẩm ứng dụng của mình.

WhiteHub cung cấp các **tính năng quản lý** trực quan, phù hợp với CEO/ CISO/CTO như:

- Tạo chương trình Bug Bounty
- Lựa chọn phạm vi thực hiện (công khai hay bí mật)
- Lựa chọn chuyên gia phù hợp
- Định nghĩa ngân sách
- Giao tiếp & trao thưởng cho chuyên gia.

>> Giải pháp Pentest thông qua Bug Bounty

3. KHÁCH HÀNG CỦA CHÚNG TÔI

Nhiều đối tác thuộc các lĩnh vực **Thương mại điện tử, Giáo dục, Y tế, Tài chính, Chứng khoán, Ví điện tử, Du lịch OTA**... đã lựa chọn WhiteHub để bảo mật cho website và ứng dụng mobile của họ:

- **vntrip.vn:** Thông qua WhiteHub, Vntrip đã kịp thời phát hiện ra những lỗ hổng hệ thống nghiêm trọng. Từ đó bảo mật thông tin cho 500,000 khách hàng và 10,000 đối tác khách sạn.
- **Getfly**
- **Luxstay**
- **NukeViet**
- **Hostvn**
- **MOG**
- **IAE**
- **...**

Đối tác nước ngoài: **GPQB, Digicentre,...**

D. TỔNG KẾT

Tội phạm mạng luôn phát triển. Việc trang bị kiến thức về bảo mật website là cần thiết với tất cả mọi người, từ cấp quản lý tới cấp nhân viên.

Tuy nhiên trong thực tế, không phải website nào cũng cần thiết phải áp dụng tất cả các phương pháp được nêu ra trong bài viết. Bạn đọc nên cân nhắc những biện pháp **phù hợp với tình hình riêng của mỗi trang web** để đưa ra chiến lược phù hợp.

Ví dụ: *Một website Thương mại điện tử (TMĐT) sẽ cần thực hiện* ***các biện pháp pentest & Bảo Mật Cộng Đồng*** *để bảo vệ tối đa cho website. Bởi trang web có vài trò rất lớn đối với công việc kinh doanh của các công ty TMĐT. Ngược lại, một website với mục đích giới thiệu về công ty thì chỉ cần thực hiện* ***các bước bảo mật website cơ bản*** *là quá đủ.*

Bài viết trên đã giúp bạn đọc trang bị thêm kiến thức về các phương pháp bảo mật website. Tuy nhiên, nếu bạn vẫn phân vân chưa biết bảo mật website như thế nào, bắt đầu từ đâu, hay chọn phương pháp nào, thì hãy liên hệ với chúng tôi để được tư vấn MIỄN PHÍ giải pháp phù hợp nhất cho doanh nghiệp của bạn.

LIÊN HỆ

CTCP An ninh mạng CyStack Việt Nam - CyStack., JSC

Địa chỉ: Bigwin Tower, Số 23 Lê Văn Lương, phường Nhân Chính, quận Thanh Xuân, Hà Nội.

Email: contact@cystack.net

Hotline: (+84) 247 109 9656

Website: **https://cystack.net**