WordPress Tiếng Việt

Code Tốt

HANOI WORDPRESS MEETUP 09/2025

BẢO MẬT WEBSITE WORDPRESS

Khôi Nguyễn

CEO & Founder - Code Tốt

Giới thiệu

CHÚNG TÔI LÀ

CHUYÊN GIA VỀ WEB

Từ kinh nghiệm với các **dự án outsourcing web development** với các thương hiệu lớn tại New York và Melbourn, Code Tốt ra đời và cung cấp dịch vụ chuyên sâu về Web Development cho **khách hàng tại Việt Nam**.

Chúng tôi tập trung vào **trải nghiệm người dùng**, **tăng tốc website**, xây dựng hệ thống **cá nhân hoá** cho mỗi doanh nghiệp trên nền tảng web.

THỰC TRẠNG

1 **Tần suất tấn công website tăng với nhiều hình thức đa dạng**

Các website bị tấn công thông qua các công cụ tự động, bị dò quét liên tục và thường xuyên bất kể ngày đêm. Hình thức tấn công đa dạng và có sự thay đổi, bao gồm cả tấn công hạ tầng, báo cáo bản quyền số.

2 **Thiệt hại nghiêm trọng**

Bao gồm thiệt hại về kinh tế (gián đoạn truy cập, gián đoạn các chương trình quảng cáo ,marketing, mất dữ liệu), thiệt hại về nhãn hiệu (thương hiệu mất uy tín)

3 **WordPress là một hệ thống phổ biến**

Với 42% website toàn cầu làm bằng WordPress, đây là một rủi ro cho mỗi website được làm từ WordPress. Mã nguồn mở, nhiều plugin và theme được phát triển bởi các bên có trình độ khác nhau, đó là cơ hội cho các hoạt động tấn công bảo mật.

Tại sao WordPress có nguy cơ BỊ TẤN CÔNG cao hơn?

MÃ NGUỒN MỞ

Mã nguồn **core** của WordPress và nhiều plugin/giao diện miễn phí là kho dữ liệu source code khổng lồ được công bố công khai.

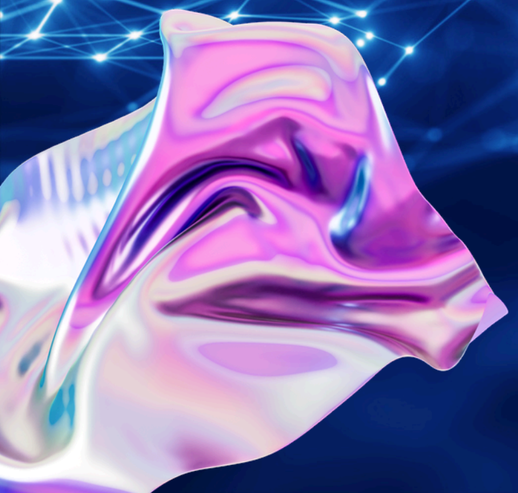
BẢN QUYỀN PHẦN MỀM

Nhiều bản quyền phần mềm trả phí được chia sẻ công khai hoặc mua bán nhưng có thể không an toàn, chứa malware.

HẠ TẦNG

Không khó để sử dụng trên các hạ tầng, nhưng rủi ro bảo mật cùng các vấn đề kỹ thuật chưa được tính đến.

Các phương pháp tấn công WordPress



Khai thác lỗ hổng phiên bản cũ

- Core WordPress
- Plugin WordPress
- Theme WordPress

Khai thác lỗ hổng phổ biến

- SQL Injection
- Tấn công DDoS
- Tấn công tài khoản quản trị
- Tấn công DNS
- Tấn công API
- Tấn công spam

PHÒNG TRÁNH TẤN CÔNG

Cài đặt 1 plugin WAF trên website

- Ninjafirewall
- Wordfence
- Solid Security
- All in one Security

BACKUP dữ liệu web và source code định kỳ

- Lưu 1 bản tại Hosting
- Lưu 1 bản tại môi trường Cloud (Google Drive, OneDrive, S3)
- Lưu 1 bản trên máy tính

Bảo trì website định kỳ

- Nâng cấp core WordPress, theme và plugin định kỳ
- Đảm bảo các tiêu chuẩn code trong quá trình sử dụng và nâng cấp web
- Tách biệt giữa source code và môi trường production
- Có bật cảnh báo website downtime, website bị tấn công lớn qua email

KHẮC PHỤC WEB
BỊ TẤN CÔNG

1. Tìm bản sao lưu dữ liệu gần nhất hoặc sạch nhất
2. Tiến hành khôi phục website lại trên một môi trường hosting/VPS khác
3. Tiến hành kiểm tra source code
    a. Kiểm tra source code core WordPress xem có sinh file lạ hoặc bị sửa không
    b. Kiểm tra các plugin và tắt các plugin nghi ngờ
    c. Kiểm tra giao diện và xem các file có thể không nằm trong cấu trúc
    d. Kiểm tra thư mục wp-content/uploads, xem có các file .PHP, .py hoặc thư mục sinh ra không giống thông thường
4. Cài trắng 1 bản WordPress mới nhất
5. Tải các bản gốc plugin chính hãng ghi vào
6. Tải các bản gốc theme chính hãng ghi vào
7. Trường hợp sử dụng giao diện viết riêng, copy tạm vào và quét luôn folder chứa theme
8. Import lại database vào và quét database thông qua các plugin như Ninja Scanner

CÁC VẤN ĐỀ KỸ THUẬT CỦA KHÔI PHỤC BACKUP WEBSITE

- Môi trường khôi phục - là Hosting/VPS mới
- Dữ liệu được tải về từ các nguồn cần có tốc độ cao, vd Google Drive, SFTP, S3
- Bản backup chứa gì?
  - Source Code
  - Database
  - File uploads
- Bản backup là định dạng gì? Increment/Full backup
- Bản backup theo cơ chế gì? Theo plugin, theo server hay script chạy tự động cronjob

KHÔI PHỤC WEBSITE BỊ HACK - KHÔNG CÓ BACKUP SẠCH

- Cài trắng 1 website WordPress với version mới nhất
- Xác định các plugin FREE có thể sử dụng và tải về từ nguồn wordpress.org
- Xác định các plugin premium mà có key chính hãng có thể tải về
- Kiểm tra thư mục uploads, đặc biệt là scan các file .htacess, file chứa PHP
- Tiến hành import database, kiểm tra các dữ liệu từ table quan trọng:
  - wp_options
  - wp_posts
  - wp_users
- Khi khôi phục, lưu ý tắt hết các tính năng update bằng admin (vd không thể tự cài theme/plugin trên admin được, không tạo mới user được)