Họ và Tên : Mai Quốc Việt

Mã Sinh Viên : 21IT595

Lớp : 21NS

Môn Học : Chuyên đề 3 (IT) (12) NS Tấn công và phòng thủ ứng dụng web

**Bài Tập**

Xây dựng quy trình kiểm tra đánh giá an toàn thông tin ứng dụng web,

Gợi ý: ít nhất phải đầy đủ 4 bước trong quy trình, vd

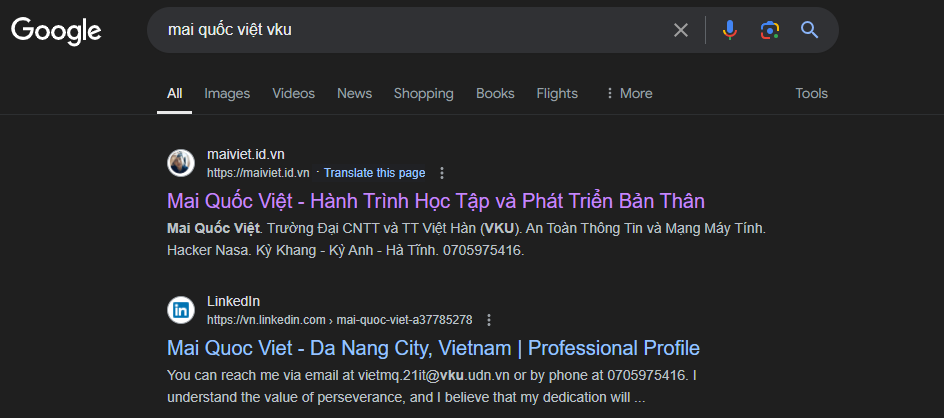
* b1 : thu thập thông tin
* b2 : rà quét lỗ hổng
* b3 : kiểm tra, khai thác lỗ hổng
* b4 : tổng hợp - báo cáo

Cụ thể : nêu rõ từng bước "làm gì ?" "công cụ" sử dụng là gì

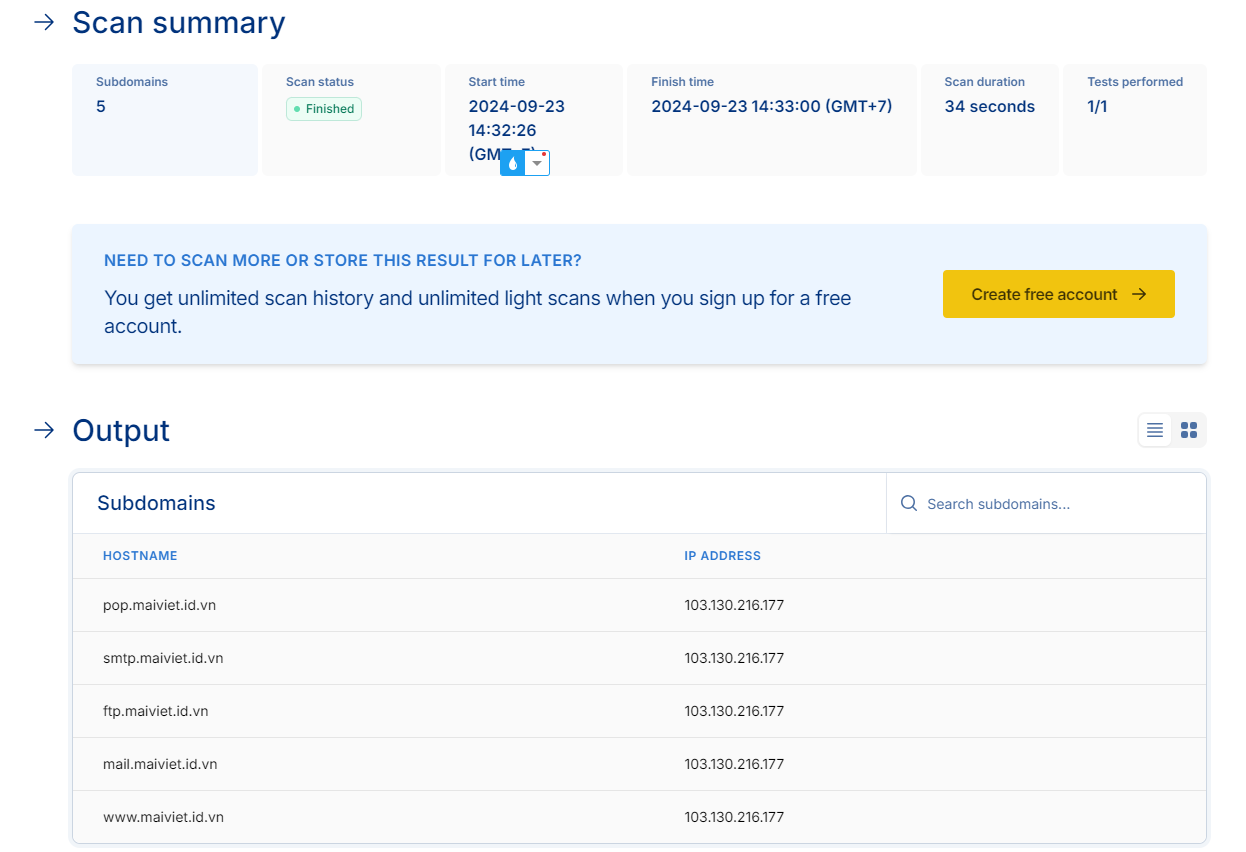
**Bài Làm**

Thu thập thông tin của trang web maiviet.id.vn

Tìm kiếm và xem trang web trên google



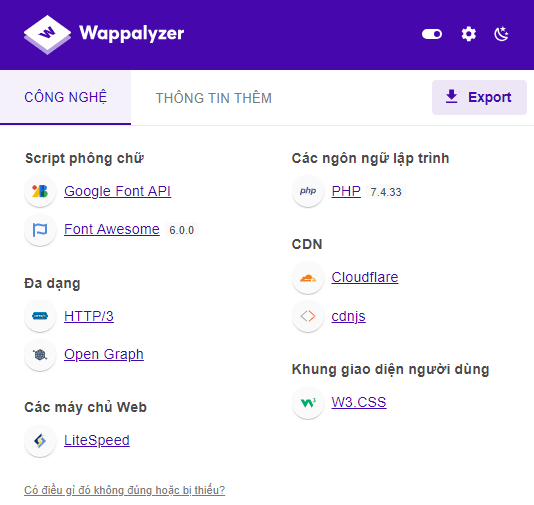
Sử dụng công cụ Pentest-tools để quét Subdomain



Các subdomains này chủ yếu liên quan đến các dịch vụ email và FTP.

* pop và smtp có thể là máy chủ thư điện tử (POP3 và SMTP).
* ftp có thể là một máy chủ FTP (File Transfer Protocol) để quản lý tập tin.
* mail có thể là tên miền chính của hệ thống mail.
* www là tên miền chính của trang web.

Sử dụng công cụ Wappalyzer để tìm hiểu công nghệ



Phông chữ: Google Font API : Dùng để quản lý và sử dụng phông chữ từ Google.

Font Awesome : Phiên bản 6.0.0: Thư viện biểu tượng cho phép sử dụng các biểu tượng trong thiết kế web.

Giao thức : HTTP/3 : Phiên bản mới nhất của giao thức HTTP, cải thiện hiệu suất và bảo mật.

Open Graph: Công nghệ giúp cải thiện việc chia sẻ nội dung trên mạng xã hội.

Máy chủ Web : LiteSpeed : Một máy chủ web hiệu suất cao, thường dùng để tối ưu hóa tốc độ tải trang.

Ngôn ngữ lập trình : PHP 7.4.33 : Phiên bản của ngôn ngữ lập trình PHP, thường được sử dụng cho phát triển web.

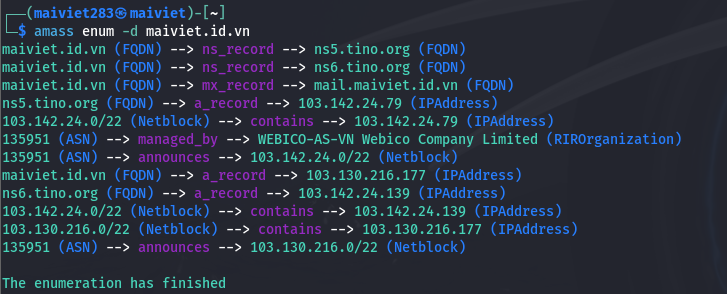
CDN (Content Delivery Network):

- Cloudflare : Dịch vụ CDN cung cấp bảo mật và tăng tốc độ tải trang.

- cdnjs : Một CDN cho phép sử dụng các thư viện JavaScript và CSS.

Khung giao diện người dùng : W3.CSS : Một khung CSS nhẹ giúp phát triển giao diện web dễ dàng hơn.

Dưới đây là tóm tắt thông tin từ quá trình quét bằng **Amass** cho trang web maiviet.id.vn:



Nameservers (NS) Records:

* ns5.tino.org – IP: 103.142.24.79
* ns6.tino.org – IP: 103.142.24.139

Nameservers này thuộc về dải IP 103.142.24.0/22 do WEBICO-AS-VN Webico Company Limited quản lý (ASN 135951).

Mail Server (MX) Record : mail.maiviet.id.vn là máy chủ mail của trang web, dùng để xử lý các dịch vụ email.

Địa chỉ IP chính của trang web : maiviet.id.vn có địa chỉ IP 103.130.216.177, nằm trong dải IP 103.130.216.0/22, cũng được quản lý bởi WEBICO-AS-VN (ASN 135951).

ASN và Netblock:

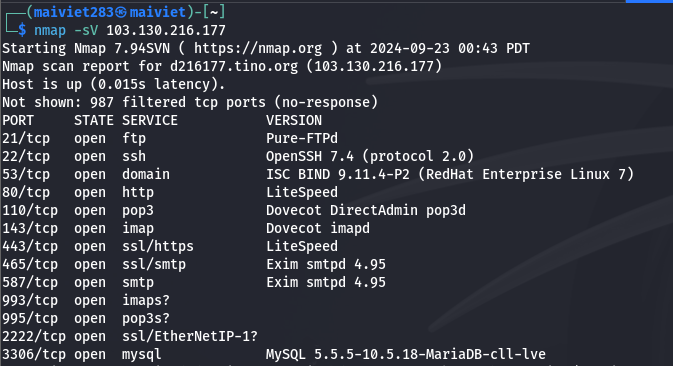
* Trang web và các nameservers thuộc ASN 135951, do WEBICO-AS-VN quản lý.
* Dải IP 103.130.216.0/22 và 103.142.24.0/22 đều nằm trong netblock được ASN này công bố và quản lý.

Ý nghĩa

- Trang web sử dụng hệ thống mạng và dịch vụ của Webico, một nhà cung cấp dịch vụ hosting tại Việt Nam.

- Tất cả các nameservers và máy chủ mail đều liên quan đến cơ sở hạ tầng của cùng một nhà cung cấp.

Sử dụng công cụ Nmap để quét IP và các cổng



1. FTP (Port 21): Máy chủ đang chạy dịch vụ Pure-FTPd.
2. SSH (Port 22): Dịch vụ OpenSSH 7.4.
3. DNS (Port 53): Dịch vụ ISC BIND 9.11.4-P2 trên hệ điều hành RedHat Enterprise Linux 7.
4. HTTP (Port 80): Máy chủ web LiteSpeed.
5. POP3 (Port 110): Dịch vụ Dovecot DirectAdmin pop3d.
6. IMAP (Port 143): Dịch vụ Dovecot imapd.
7. HTTPS (Port 443): Máy chủ web LiteSpeed hỗ trợ SSL.
8. SMTP (Ports 465 và 587): Dịch vụ Exim smtpd 4.95.
9. MySQL (Port 3306): Phiên bản MySQL 5.5.5-10.5.18-MariaDB-cll-lve.