WebSec - Thực Hành Buổi 4

Mở đầu

Reconnaissance là quá trình thu thập thông tin về tổ chức hoặc hệ thống thông tin mục tiêu, đây là một phần quan trọng trong penetration testing và bug bounty hunting khi mà thông tin về target chỉ được cung cấp 1 phần hoặc không được cung cấp.

Mục tiêu của quá trình reconnaissance (từ giờ sẽ gọi ngắn gọn là recon) là thu thập càng nhiều thông tin về đối tượng càng tốt, từ đó pentester có thể xác định được các điểm yếu tiềm ẩn để thực hiện khai thác. Thực hiện tốt Recon giúp pentester hiểu rõ về đối tượng và mở rộng **attack surface**. Các thông tin sẽ là không giới hạn, tuỳ thuộc đối tượng đó là gì và cách tận dụng các thông tin có được để khai thác đối tượng. Các thông tin cơ bản nhất cần được thu thập mình đã đề cập đến trong slide phần Reconnaissance dựa trên scope đang thực hiện.

Trong bài này mình sẽ giới thiệu về một số tools dùng trong quá trình Recon và kết hợp tools để automation recon cơ bản. Scope ở đây mình đang giả định thực hiện tìm lỗi trên các subdomain của funix.edu.vn .

Tổng quan về công cụ sử dụng

Prerequisite: các tool đề cập trong bài này được code bằng Go, chúng ta cần install Go để có thể sử dụng được tools. Cài đặt Go tham khảo tại https://go.dev/doc/install

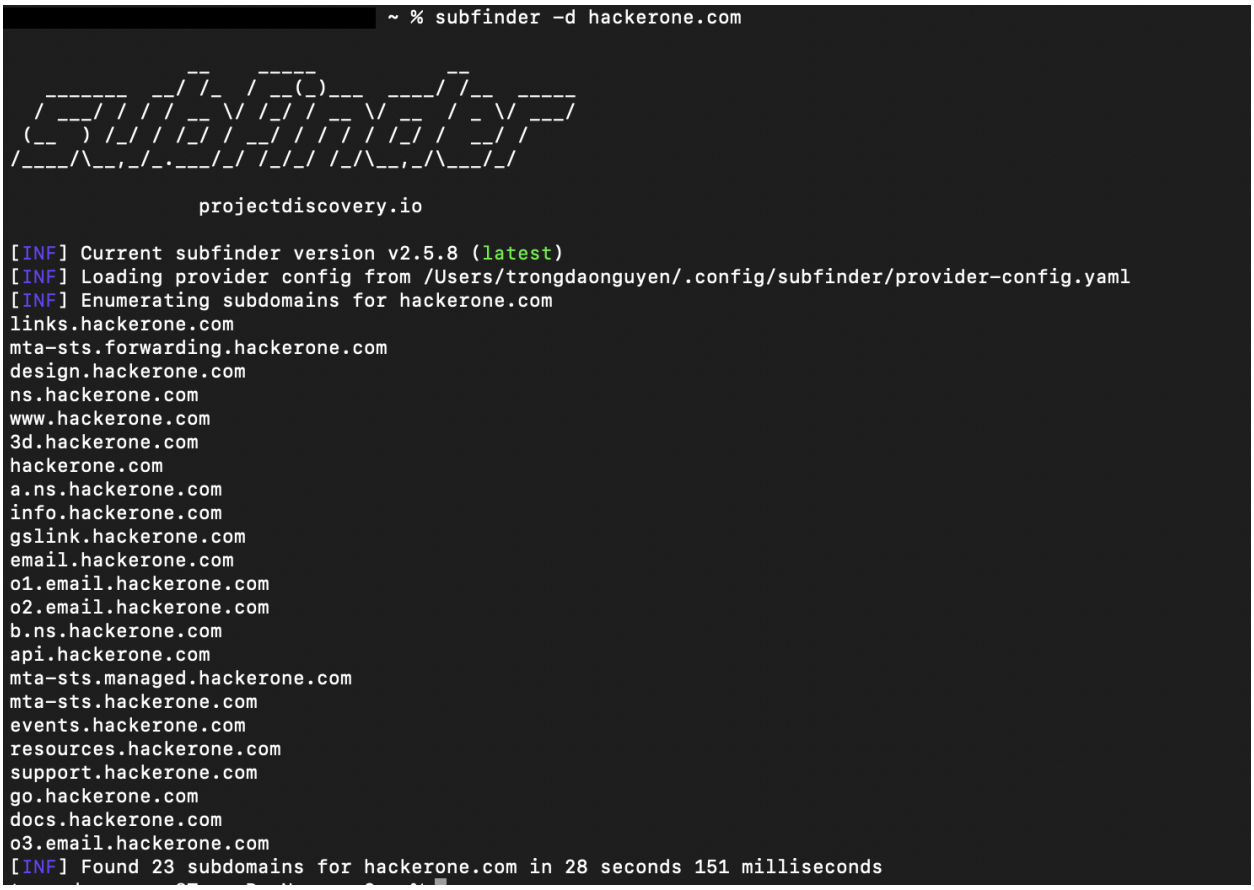
Subfinder

subfinder là công cụ dùng để enumerate subdomain được viết bằng ngôn ngữ lập trình Go. Công cụ sẽ trả về các subdomain hợp lệ sử dụng thông tin từ các nguồn khác (Chaos, Shodan, ZoomEye…). Chi tiết về subfinder: https://github.com/projectdiscovery/subfinder#features

Để dùng subfinder một cách cơ bản nhất, chạy command sau trên terminal.

```
subfinder -d hackerone.com
```

`-d` là flag chỉ định domain mình muốn tìm subdomain



Kết quả ta có thể thấy subfinder tìm được **23** subdomains của hackerone.com

Sử dụng `-v` flag để xem chi tiết output của subfinder, ta có thể thấy được các nguồn được dùng để enumerate subdomain.

```
[digitorus] info.hackerone.com
[digitorus] mta-sts.managed.hackerone.com
[digitorus] support.hackerone.com
[digitorus] mta-sts.forwarding.hackerone.com
[digitorus] mta-sts.hackerone.com
[digitorus] gslink.hackerone.com
[digitorus] design.hackerone.com
[digitorus] events.hackerone.com
[chaos] a.ns.hackerone.com
[chaos] api.hackerone.com
[chaos] b.ns.hackerone.com
[chaos] design.hackerone.com
[chaos] docs.hackerone.com
[chaos] email.hackerone.com
[chaos] events.hackerone.com
[chaos] go.hackerone.com
[chaos] gslink.hackerone.com
[chaos] info.hackerone.com
[chaos] links.hackerone.com
```

Httpx

httpx là công cụ cho phép thu thập thông tin về web server. Thông tin này có thể giúp xác định các lỗ hổng và điểm yếu trên máy chủ. Httpx có nhiều option khác nhau để tìm những subdomain alive, xem các response header, xác định HTTP methods…

Chi tiết về httpx: https://github.com/projectdiscovery/httpx

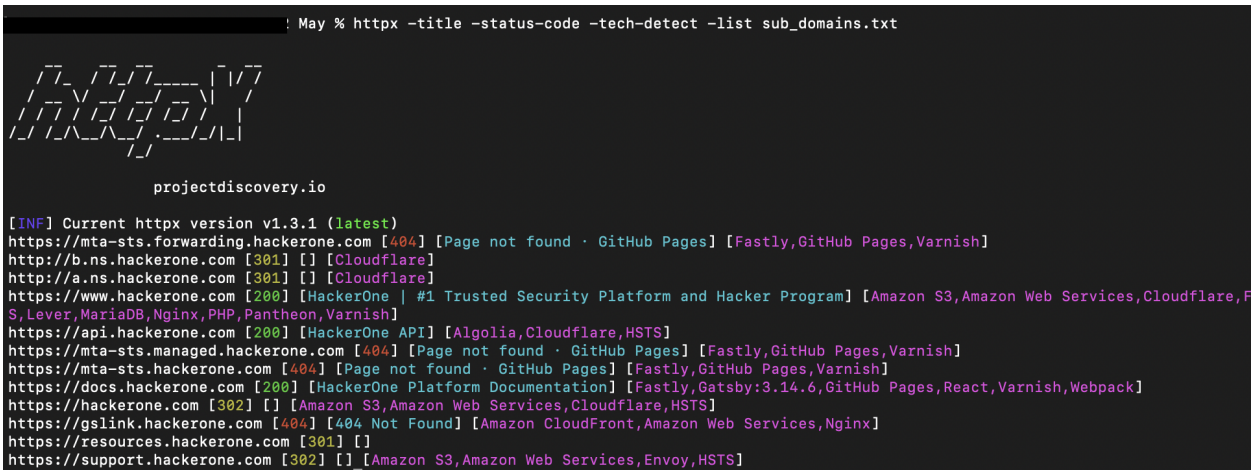
Command: `httpx -status-code -tech-detect -title -list sub_domains.txt`

`-status-code` được sử dụng để show ra status code khi mà request đến subdomain

`-tech-detect` cho phép xác định công nghệ & framework được sử dụng

`-title` extract title của webpage từ source code HTML

`-list` chỉ ra file chứa các subdomain mà mình thu thập được



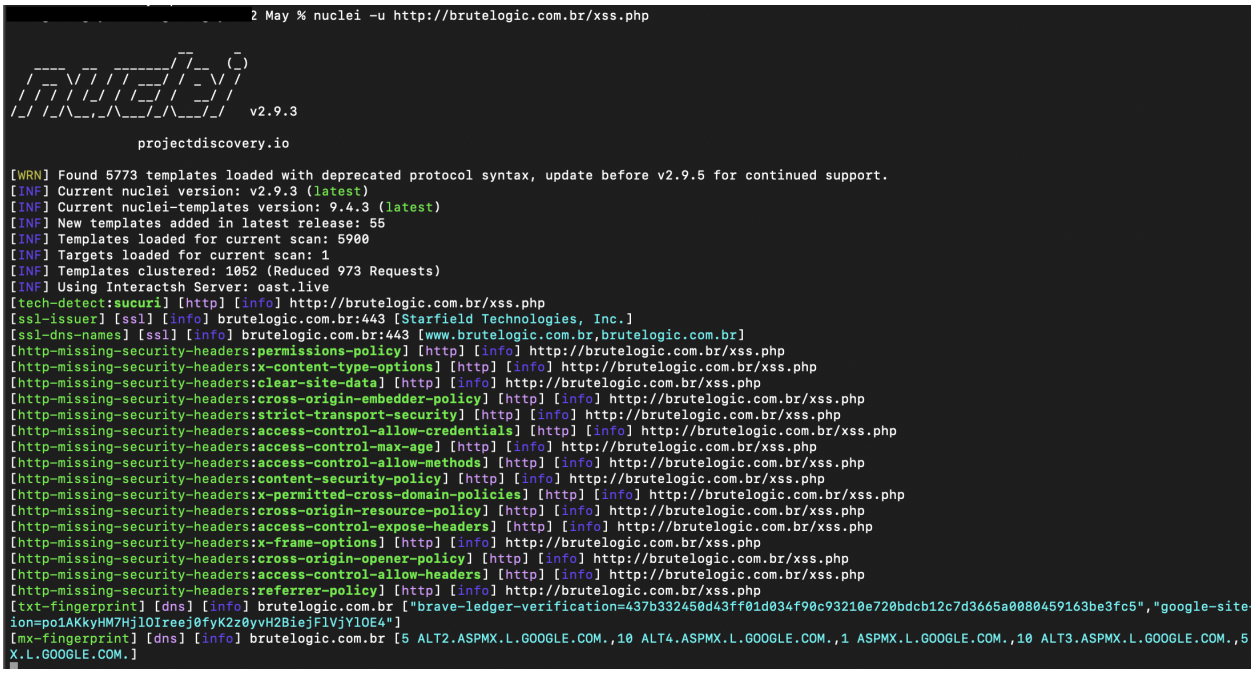
Nuclei

nuclei là công cụ sử dụng để tự động scan các lỗ hổng và thu thập thông tin (tuỳ thuộc vào option mà mọi người chỉ định)

Chi tiết về nuclei: https://github.com/projectdiscovery/nuclei

Command: nuclei -u http://brutelogic.com.br/xss.php

`-u` chỉ định url của target muốn scan

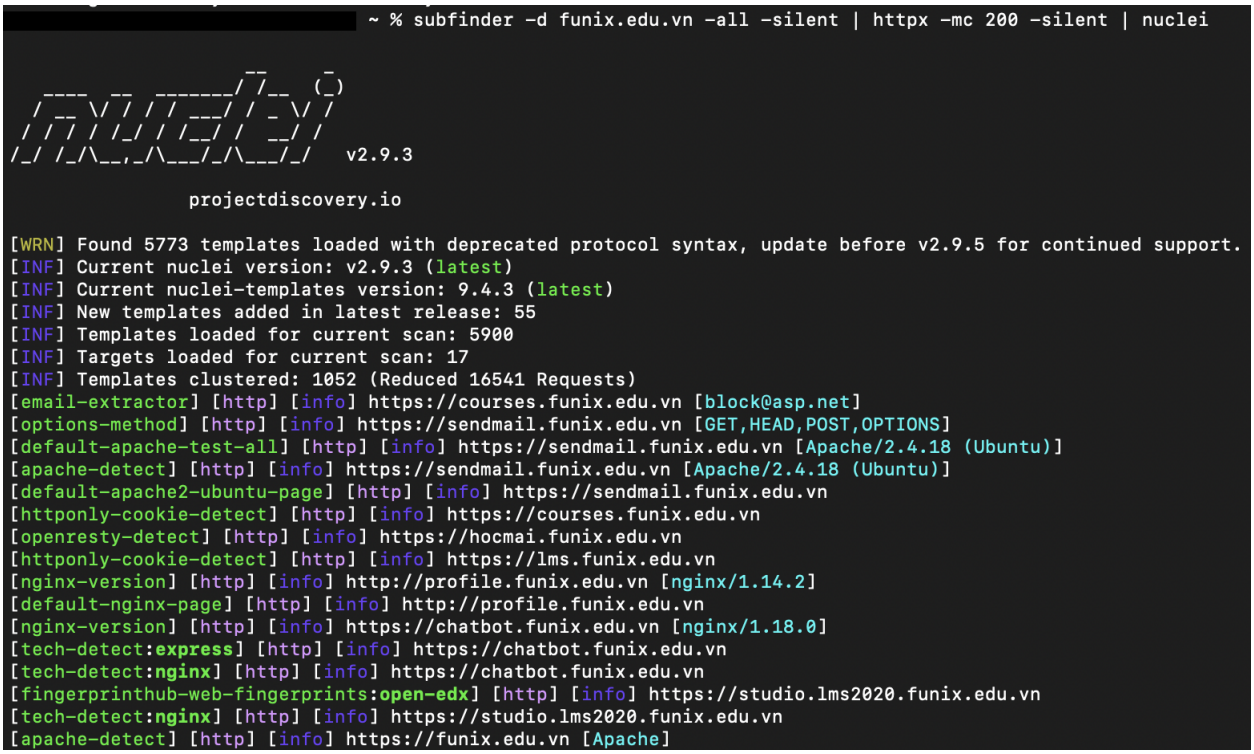


Put it together

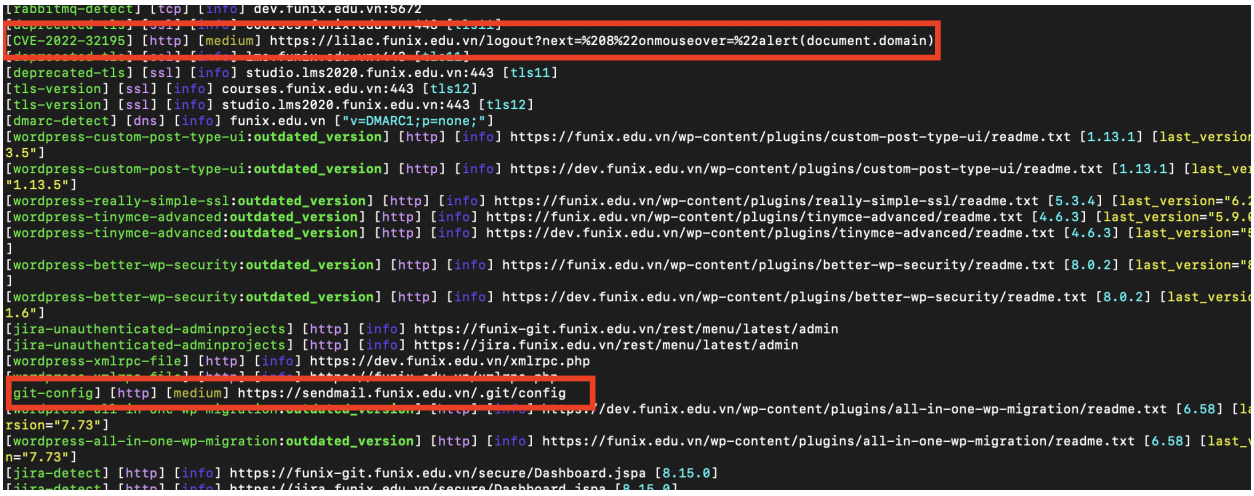
Phần trên mình đã giới thiệu tổng quan về tool và cách sử dụng, trong phần này mình sẽ kết hợp 3 tools lại với nhau để tạo một workflow recon cơ bản nhất. Workflow này sẽ có 3 stage:

- stage 1: sử dụng subfinder để tìm các subdomain của một domain mình muốn pentest.
- stage 2: do subfinder sử dụng passive recon, lấy thông tin từ các nguồn khác nên có thể kết quả trả về sẽ bao gồm những subdomain đã cũ và hiện tại không còn được sử dụng, nên giai đoạn này mình sẽ sử dụng httpx để lọc ra subdomains đang hoạt động.
- stage 3: cuối cùng sẽ sử dụng nuclei để tìm ra các folder, CVEs, fuzzing input,… Mục đích là tìm lỗi một cách tự động.

Kết hợp 3 tool lại thành one-line command như sau: `subfinder -d funix.edu.vn -all -silent | httpx -mc 200 -silent | nuclei`



Ta có thể thấy một số thông tin thú vị mà tool phát hiện ra:



Kết luận

Các tool mình đề cập còn nhiều option khác để các bạn khám phá. Để tận dụng được các tool này một cách hiệu quả, các bạn nên tìm hiểu các tính năng mà công cụ hỗ trợ. Xem tất cả options của tool bằng cách gõ command: `<tool> -h`, ví dụ: `nuclei -h`

Workflow Recon mình nêu ở trên chỉ là workflow cơ bản nhất, mọi người có thể phát triển thêm các stage khác, kết hợp thêm nhiều tool nữa. Đây là một số ý kiến của mình về việc phát triển thêm:

1. Tại stage enumerate subdomain có thể kết hợp thêm tool khác như `amass`, và kết hợp kỹ thuật active enumerate subdomain, sử dụng tool `dnsx`, `puredns` để tìm ra tối đa subdomain.
2. Phát triển thêm stage thu thập các Url có trên từng target cụ thể, sử dụng `katana` hoặc `gau` (getallurls) để tìm ra những tính năng ẩn hoặc lọc ra các url nhận tham số rồi từ đó chạy tools scan lỗi cụ thể như `sqlmap`, `dalfox`, …
3. Tự động Screenshot lại các trang web để xác định các mục tiêu tiềm năng từ đó thực hiện manual testing.