

# 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, tùy 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](https://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

```
~ % subfinder -d hackerone.com

      _ _ _ _ _
     / / / / /
    / / / / /
   / / / / /
  / / / / /
 / / / / /
/ / / / /

projectdiscovery.io

[INF] Current subfinder version v2.5.8 (latest)
[INF] Loading provider config from /Users/trongdaonguyen/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for hackerone.com
links.hackerone.com
mta-sts.forwarding.hackerone.com
design.hackerone.com
ns.hackerone.com
www.hackerone.com
3d.hackerone.com
hackerone.com
a.ns.hackerone.com
info.hackerone.com
gslink.hackerone.com
email.hackerone.com
o1.email.hackerone.com
o2.email.hackerone.com
b.ns.hackerone.com
api.hackerone.com
mta-sts.managed.hackerone.com
mta-sts.hackerone.com
events.hackerone.com
resources.hackerone.com
support.hackerone.com
go.hackerone.com
docs.hackerone.com
o3.email.hackerone.com
[INF] Found 23 subdomains for hackerone.com in 28 seconds 151 milliseconds
```

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

```
May % httpx -title -status-code -tech-detect -list sub_domains.txt

projectdiscovery.io

[INF] Current httpx version v1.3.1 (latest)
https://mta-sts.forwarding.hackerone.com [404] [Page not found · GitHub Pages] [Fastly,GitHub Pages,Varnish]
http://b.ns.hackerone.com [301] [] [Cloudflare]
http://a.ns.hackerone.com [301] [] [Cloudflare]
https://www.hackerone.com [200] [HackerOne | #1 Trusted Security Platform and Hacker Program] [Amazon S3,Amazon Web Services,Cloudflare,F
S,Lever,MariaDB,Ngix,PHP,Pantheon,Varnish]
https://api.hackerone.com [200] [HackerOne API] [Algolia,Cloudflare,HSTS]
https://mta-sts.managed.hackerone.com [404] [Page not found · GitHub Pages] [Fastly,GitHub Pages,Varnish]
https://mta-sts.hackerone.com [404] [Page not found · GitHub Pages] [Fastly,GitHub Pages,Varnish]
https://docs.hackerone.com [200] [HackerOne Platform Documentation] [Fastly,Gatsby:3.14.6,GitHub Pages,React,Varnish,Webpack]
https://hackerone.com [302] [] [Amazon S3,Amazon Web Services,Cloudflare,HSTS]
https://gslink.hackerone.com [404] [404 Not Found] [Amazon CloudFront,Amazon Web Services,Ngix]
https://resources.hackerone.com [301] []
https://support.hackerone.com [302] [] [Amazon S3,Amazon Web Services,Envoy,HSTS]
```

## Nuclei

nuclei là công cụ sử dụng để tự động scan các lỗ hổng và thu thập thông tin (tùy 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

```
2 May % nuclei -u http://brutelogic.com.br/xss.php

  _____
 /  _  _  _  \
|  _ \| | | | | | |
| |_) | | | | |
|  _ \| | | | |
|_| \_|_|_|_|_|
v2.9.3

projectdiscovery.io

[WRN] Found 5773 templates loaded with deprecated protocol syntax, update before v2.9.5 for continued support.
[INF] Current nuclei version: v2.9.3 (latest)
[INF] Current nuclei-templates version: 9.4.3 (latest)
[INF] New templates added in latest release: 65
[INF] Templates loaded for current scan: 5900
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 1052 (Reduced 973 Requests)
[INF] Using Interactsh Server: oast.live
[tech-detect:sucuri] [http] [info] http://brutelogic.com.br/xss.php
[ssl-issuer] [ssl] [info] brutelogic.com.br:443 [Starfield Technologies, Inc.]
[ssl-dns-names] [ssl] [info] brutelogic.com.br:443 [www.brutelogic.com.br,brutelogic.com.br]
[http-missing-security-headers:permissions-policy] [http] [info] http://brutelogic.com.br/xss.php
[http-missing-security-headers:x-content-type-options] [http] [info] http://brutelogic.com.br/xss.php
[http-missing-security-headers:clear-site-data] [http] [info] http://brutelogic.com.br/xss.php
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://brutelogic.com.br/xss.php
[http-missing-security-headers:strict-transport-security] [http] [info] http://brutelogic.com.br/xss.php
[http-missing-security-headers:access-control-allow-credentials] [http] [info] http://brutelogic.com.br/xss.php
[http-missing-security-headers:access-control-max-age] [http] [info] http://brutelogic.com.br/xss.php
[http-missing-security-headers:access-control-allow-methods] [http] [info] http://brutelogic.com.br/xss.php
[http-missing-security-headers:content-security-policy] [http] [info] http://brutelogic.com.br/xss.php
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://brutelogic.com.br/xss.php
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://brutelogic.com.br/xss.php
[http-missing-security-headers:access-control-expose-headers] [http] [info] http://brutelogic.com.br/xss.php
[http-missing-security-headers:x-frame-options] [http] [info] http://brutelogic.com.br/xss.php
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://brutelogic.com.br/xss.php
[http-missing-security-headers:access-control-allow-headers] [http] [info] http://brutelogic.com.br/xss.php
[http-missing-security-headers:referrer-policy] [http] [info] http://brutelogic.com.br/xss.php
[txt-fingerprint] [dns] [info] brutelogic.com.br ["brave-ledger-verification=437b332450d43ff0d034f90c93210e720bdc12c7d3665a0080459163be3fc5", "google-site-
ion=po1AKkyHM7Hj10Ireej0fyK2zyvH2BiejF1VjY10E4"]
[mx-fingerprint] [dns] [info] brutelogic.com.br [5 ALT2.ASPMX.L.GOOGLE.COM.,10 ALT4.ASPMX.L.GOOGLE.COM.,1 ASPMX.L.GOOGLE.COM.,10 ALT3.ASPMX.L.GOOGLE.COM.,5
X.L.GOOGLE.COM.]
```

## 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`



```
~ % subfinder -d funix.edu.vn -all -silent | httpx -mc 200 -silent | nuclei

projectdiscovery.io

[WRN] Found 5773 templates loaded with deprecated protocol syntax, update before v2.9.5 for continued support.
[INF] Current nuclei version: v2.9.3 (latest)
[INF] Current nuclei-templates version: 9.4.3 (latest)
[INF] New templates added in latest release: 55
[INF] Templates loaded for current scan: 5900
[INF] Targets loaded for current scan: 17
[INF] Templates clustered: 1052 (Reduced 16541 Requests)
[email-extractor] [http] [info] https://courses.funix.edu.vn [block@asp.net]
[options-method] [http] [info] https://sendmail.funix.edu.vn [GET,HEAD,POST,OPTIONS]
[default-apache-test-all] [http] [info] https://sendmail.funix.edu.vn [Apache/2.4.18 (Ubuntu)]
[apache-detect] [http] [info] https://sendmail.funix.edu.vn [Apache/2.4.18 (Ubuntu)]
[default-apache2-ubuntu-page] [http] [info] https://sendmail.funix.edu.vn
[httponly-cookie-detect] [http] [info] https://courses.funix.edu.vn
[openresty-detect] [http] [info] https://hocmai.funix.edu.vn
[httponly-cookie-detect] [http] [info] https://lms.funix.edu.vn
[nginx-version] [http] [info] http://profile.funix.edu.vn [nginx/1.14.2]
[default-nginx-page] [http] [info] http://profile.funix.edu.vn
[nginx-version] [http] [info] https://chatbot.funix.edu.vn [nginx/1.18.0]
[tech-detect:express] [http] [info] https://chatbot.funix.edu.vn
[tech-detect:nginx] [http] [info] https://chatbot.funix.edu.vn
[fingerprinthub-web-fingerprints:open-edx] [http] [info] https://studio.lms2020.funix.edu.vn
[tech-detect:nginx] [http] [info] https://studio.lms2020.funix.edu.vn
[apache-detect] [http] [info] https://funix.edu.vn [Apache]
```

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

```
[rabbitmq-detect] [tcp] [info] dev.funix.edu.vn:5672
[deprecated-tls] [ssl] [info] courses.funix.edu.vn:443 [tls11]
[CVE-2022-32195] [http] [medium] https://lilac.funix.edu.vn/logout?next=%208%22onmouseover=%22alert(document.domain)
[deprecated-tls] [ssl] [info] studio.lms2020.funix.edu.vn:443 [tls12]
[deprecated-tls] [ssl] [info] courses.funix.edu.vn:443 [tls12]
[deprecated-tls] [ssl] [info] studio.lms2020.funix.edu.vn:443 [tls12]
[dmARC-detect] [dns] [info] funix.edu.vn ["v=DMARC1;p=none;"]
[wordpress-custom-post-type-ui:outdated_version] [http] [info] https://funix.edu.vn/wp-content/plugins/custom-post-type-ui/readme.txt [1.13.1] [last_version=3.5]
[wordpress-custom-post-type-ui:outdated_version] [http] [info] https://dev.funix.edu.vn/wp-content/plugins/custom-post-type-ui/readme.txt [1.13.1] [last_version=1.13.5]
[wordpress-really-simple-ssl:outdated_version] [http] [info] https://funix.edu.vn/wp-content/plugins/really-simple-ssl/readme.txt [5.3.4] [last_version="6.7"]
[wordpress-tinymce-advanced:outdated_version] [http] [info] https://funix.edu.vn/wp-content/plugins/tinymce-advanced/readme.txt [4.6.3] [last_version="5.9.6"]
[wordpress-tinymce-advanced:outdated_version] [http] [info] https://dev.funix.edu.vn/wp-content/plugins/tinymce-advanced/readme.txt [4.6.3] [last_version="5.9.6"]
[wordpress-better-wp-security:outdated_version] [http] [info] https://funix.edu.vn/wp-content/plugins/better-wp-security/readme.txt [8.0.2] [last_version="8.1.6"]
[wordpress-better-wp-security:outdated_version] [http] [info] https://dev.funix.edu.vn/wp-content/plugins/better-wp-security/readme.txt [8.0.2] [last_version="8.1.6"]
[jira-unauthenticated-adminprojects] [http] [info] https://funix-git.funix.edu.vn/rest/menu/latest/admin
[jira-unauthenticated-adminprojects] [http] [info] https://jira.funix.edu.vn/rest/menu/latest/admin
[wordpress-xmlrpc-file] [http] [info] https://dev.funix.edu.vn/xmlrpc.php
[wordpress-xmlrpc-file] [http] [info] https://funix.edu.vn/xmlrpc.php
[git-config] [http] [medium] https://sendmail.funix.edu.vn/.git/config
[wordpress-all-in-one-wp-migration:outdated_version] [http] [info] https://dev.funix.edu.vn/wp-content/plugins/all-in-one-wp-migration/readme.txt [6.58] [last_version="7.73"]
[wordpress-all-in-one-wp-migration:outdated_version] [http] [info] https://funix.edu.vn/wp-content/plugins/all-in-one-wp-migration/readme.txt [6.58] [last_version="7.73"]
[jira-detect] [http] [info] https://funix-git.funix.edu.vn/secure/Dashboard.jspa [8.15.0]
[jira-detect] [http] [info] https://jira.funix.edu.vn/secure/Dashboard.jspa [8.15.0]
```

## 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.