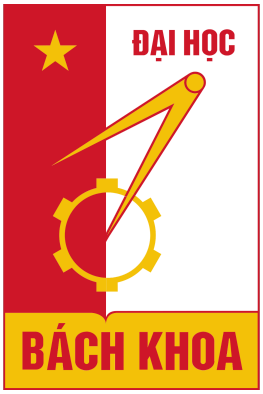
HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY
SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY



PROJECT 2

Reconnaissance Tool

Instructor: Dr. Tran Quang Duc
Student: Le Duc Dung - 20214952

HANOI - JUNE 2024

TABLE OF CONTENTS

1 Introduction

1.1 Brief Overview

The primary goal of this project RecoNess is to develop an integrated reconnaissance tool that combines the functionalities of ffuf, nmap, dirsearch, and CVE searching to enhance the efficiency and effectiveness of penetration testing efforts. By automating and unifying these tools, the project aims to streamline the process of gathering critical information about target systems and identifying potential vulnerabilities.

1.2 Key Objectives

Reconnaissance is one of the most important step in an attack scenario. As the hackers' skills field is getting closer and closer to each other, more attack surfaces will make a big difference in finding vulnerabilities or not. Reconnaissance is too big to be combined in one go but with this tool will help combining some famous and essential tools make pentester and redteamer easier to do their work and maybe improve testing efficiency.

1.3 Definitions, Acronyms, and Abbreviations

- CLI: Command Line Interface
- CVE: Common Vulnerabilities and Exposures
- CWE: Common Weakness Enumeration

1.4 References

- FFUF: `https://github.com/ffuf/ffuf`
- Dirsearch: `https://github.com/maurosoria/dirsearch`
- Nmap: `https://github.com/nmap/nmap`
- Arjun: `https://github.com/s0md3v/Arjun`
- Whatweb: `https://github.com/urbanadventurer/WhatWeb`
- NVD CVE Database: `https://nvd.nist.gov/`

2 Tools

2.1 FFUF (Fuzz Faster U Fool)

2.1.1 Description

FFUF (Fuzz Faster U Fool) is a web fuzzing tool designed to find hidden files, directories, and parameters on web servers. It's commonly used in penetration testing and security assessments to discover potential vulnerabilities and misconfigurations.But in this project ffuf only serve the subdomain fuzzing.

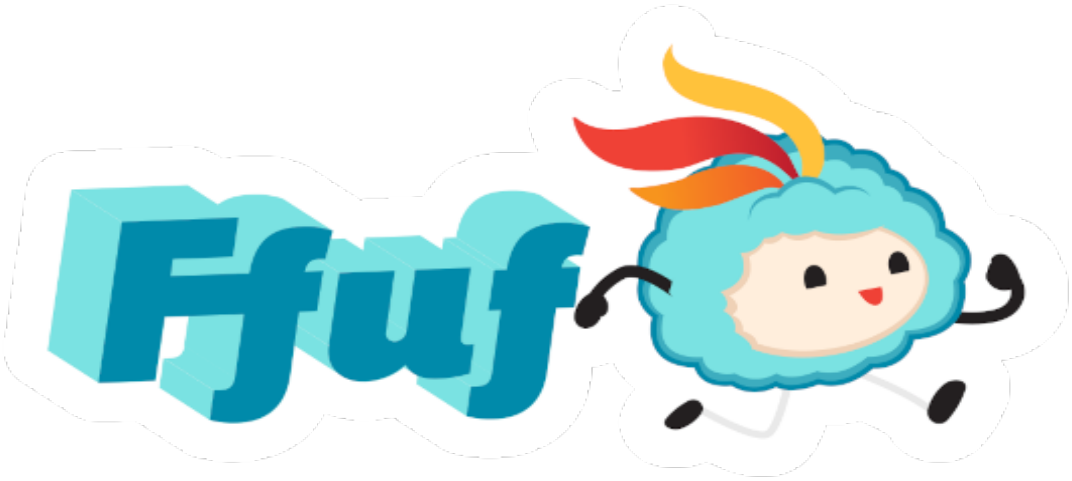


Figure 1: **FFUF**

2.1.2 Key Features

- High-speed fuzzing.
- Multiple input modes: wordlist, range, and stdin.
- Flexible output formats: JSON, HTML, and Markdown.
- Supports recursive fuzzing, HTTP/HTTPS, and POST requests.

2.1.3 Usage

In this picture, I'm running a subdomain scan on website `https://kenh14.vn` using these flag

- -u: Target URL (Include the FUZZ keyword inside the URL)
- -w: Wordlist directory
- -t: Number of threads (Default: 40)

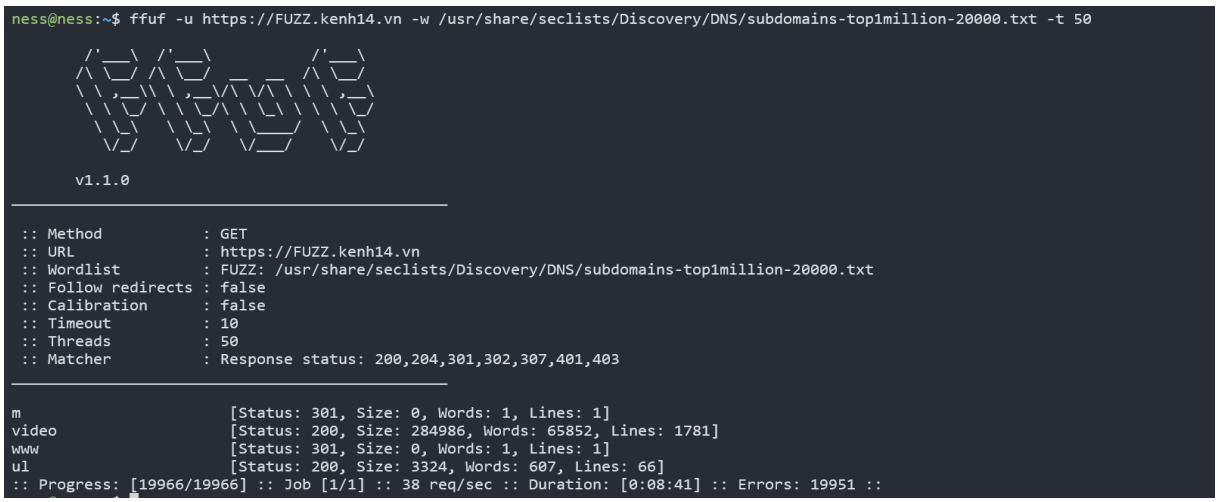


Figure 2: **Subdomain Scanning**

2.2 Dirsearch

2.2.1 Description

Dirsearch is a command-line tool used for web path scanning. It's designed to help security professionals and penetration testers find hidden directories and files on web servers. By using wordlists and performing brute-force attacks, Dirsearch can discover resources that are not publicly linked but may be accessible and potentially vulnerable.

Figure 3: **Dirsearch**

2.2.2 Key Features

- Supports multiple file extensions and HTTP methods.
- Allows recursive brute-forcing.
- Customizable wordlists.

2.2.3 Usage

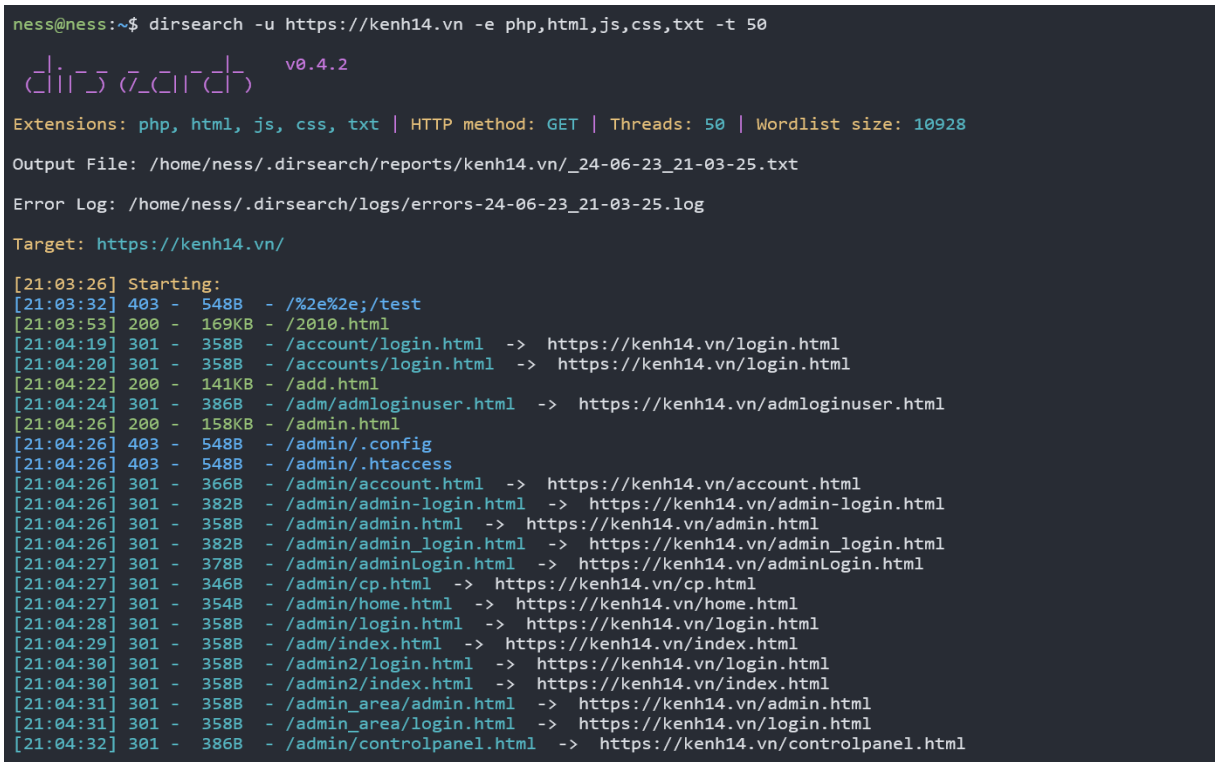


Figure 4: **Directory Scanning**

In this picture, I'm running a directory scan on website `https://kenh14.vn` using these flag

- -u: Target URL
- -e: Extension lists
- -t: Number of threads

2.3 Nmap

2.3.1 Description

Nmap (Network Mapper) is a popular open-source tool used for network discovery and security auditing. It helps users map out a network, identify active devices, and gather information about the services running on these devices.

Figure 5: **Nmap**

2.3.2 Key Features

- Finds active devices on a network.
- Identifies open ports and the services running on them.
- Determines the version of the service running on a port.
- Guesses the operating system of a device.
- Uses scripts to detect security vulnerabilities.
- Produces results in various formats for analysis.

2.3.3 Usage

```
ness@ness:~$ sudo nmap -O -sS -sV 127.0.0.1 -v
Starting Nmap 7.80 ( https://nmap.org ) at 2024-06-23 21:38 +07
NSE: Loaded 45 scripts for scanning.
Initiating SYN Stealth Scan at 21:38
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 3306/tcp on 127.0.0.1
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 5432/tcp on 127.0.0.1
Completed SYN Stealth Scan at 21:38, 0.07s elapsed (1000 total ports)
Initiating Service scan at 21:38
Scanning 3 services on localhost (127.0.0.1)
Completed Service scan at 21:38, 6.02s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against localhost (127.0.0.1)
NSE: Script scanning 127.0.0.1.
Initiating NSE at 21:38
Completed NSE at 21:38, 0.00s elapsed
Initiating NSE at 21:38
Completed NSE at 21:38, 0.00s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000028s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE     VERSION
80/tcp   open  http        Apache httpd 2.4.52 ((Ubuntu))
3306/tcp open  nagios-nsca Nagios NSCA
5432/tcp open  postgresql  PostgreSQL DB 9.6.0 or later
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.c
gi?new-service :
SF-Port5432-TCP:V=7.80%I=7%D=6/23%Time=66783376%P=x86_64-pc-linux-gnu%r(SM
SF:BProgNeg,8C,"E\0\0\0\x8bSFATAL\0VFATAL\0C0A000\0Munsupported\x20fronten
SF:d\x20protocol\x2065363\.19778:\x20server\x20supports\x203\.0\x20to\x203
SF:\.0\0Fpostmaster\.c\0L2142\0RProcessStartupPacket\0\0");
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
```

Figure 6: **Port Scanning**

In this picture, I'm running a port scan on localhost `127.0.0.1` using these flag

- -O: OS scan

- -sS: Stealth scan
- -sV: Service version
- -v: Verbose output

2.4 Arjun

2.4.1 Description

Arjun is a command-line tool designed to help security researchers and penetration testers discover hidden GET and POST parameters in web applications. It's particularly useful for identifying parameters that might be vulnerable to attacks like SQL injection, XSS, or other web vulnerabilities.

Figure 7: **Arjun**

2.4.2 Key Features

- Finds active devices on a network.
- Identifies open ports and the services running on them.
- Determines the version of the service running on a port.
- Guesses the operating system of a device.
- Uses scripts to detect security vulnerabilities.
- Produces results in various formats for analysis.

2.4.3 Usage

Figure 8: **Parameters Scanning**

In this picture, I'm running a parameters scan on `https://kenh14.vn` using these flag

- -O: OS scan
- -sS: Stealth scan
- -sV: Service version
- -v: Verbose output

2.5 Whatweb

2.5.1 Description

WhatWeb is a web scanner designed to identify technologies used on websites. It helps security researchers, penetration testers, and developers gather detailed information about web applications.

Figure 9: **Whatweb**

2.5.2 Key Features

- Technology Detection: Identifies web technologies such as content management systems (CMS), frameworks, programming languages, web servers, and database types.

- Plugin System: Uses a wide range of plugins to recognize specific technologies and extract detailed information.
- Stealthy Scanning: Offers options for both stealthy, low-profile scanning and more aggressive, detailed scanning.
- Output Options: Provides various output formats (text, JSON, XML) for easy analysis and reporting.
- Extensible: Allows users to create custom plugins to enhance detection capabilities.

2.5.3 Usage

Figure 10: **Technologies Scanning**

In this picture, I'm running a technologies scan on website `kenh14.vn` using these flag

- -u: Target URL
- -e: Extension lists
- -t: Number of threads

2.6 CVE Search

2.6.1 Description

CVE Search is a tool created to help with searching for CVE in NVD database using API. Each CVE gives information such as CVE name, CVE ID, References, Source, CVSS metrics, Time ublished, Vuln status, Weaknesses.

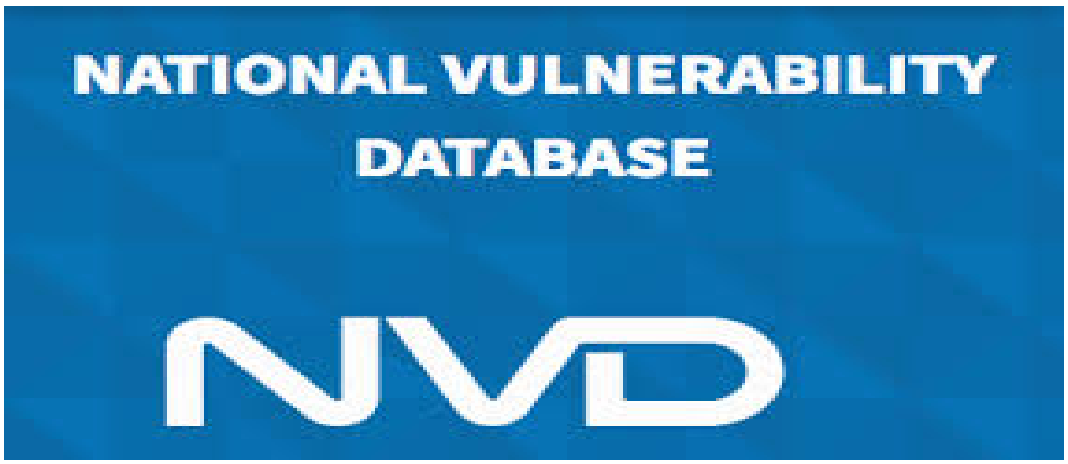


Figure 11: **NVD**

2.6.2 Key Features

- List database related to a keyword
- Finding many informations about a specific CVE

2.6.3 Usage

In this picture, I'm finding a CVE about "openresty" - Which is the web server of `https://kenh14.vn`.

```
Enter id of the CVE you want to search:CVE-2018-9230
Descriptions:
  Language: en
  Value: In OpenResty through 1.13.6.1, URI parameters are obtained using the ngx.req.get_uri_args and ngx.req.get_post_args functions that ignore parameters beyond the hundredth one, which might allow remote a
ttackers to bypass intended access restrictions or interfere with certain Web Application Firewall (ngx_lua_waf or X-WAF) products. NOTE: the vendor has reported that 100 parameters is an intentional default se
tting, but is adjustable within the API. The vendor's position is that a security-relevant misuse of the API by a WAF product is a vulnerability in the WAF product, not a vulnerability in OpenResty
  Language: es
  Value: ** EN DISPUTA** En OpenResty hasta la versión 1.13.6.1, los parámetros URI se obtienen utilizando las funciones ngx.req.get_uri_args y ngx.req.get_post_args que ignoran los parámetros posteriores al ce
ntésimo, lo que permite que los atacantes omitan las restricciones de acceso o interfieran con determinados productos Web Application Firewall (ngx_lua_waf o X-WAF). NOTA: el fabricante ha notificado que 100 pa
rámetros es una configuración por defecto intencional, pero puede ajustarse en la API. La postura del fabricante es que un uso erróneo relevante para las seguridad de la API por parte de un producto WAF es una
vulnerabilidad del producto WAF, no en OpenResty.
References:
  URL: https://github.com/Bypass007/vuln/blob/master/OpenResty/Uri%20parameter%20overflow%20in%20Openresty.md
  Source: cve@mitre.org
  Tags: Exploit, Third Party Advisory
  URL: https://openresty.org/en/changelog-1013006.html
  Source: cve@mitre.org
  Tags: Vendor Advisory
CVE ID: CVE-2018-9230
Source Identifier: cve@mitre.org
Published: 2018-04-02T18:29:00.233
Last Modified: 2024-05-17T01:30:23.610
Vulnerability Status: Modified
Weaknesses:
  Source: nvd@nist.gov
  Type: Primary
  Description: [{'lang': 'en', 'value': 'CWE-89'}]
Configurations:
  Nodes: [{'operator': 'OR', 'negate': False, 'cpeMatch': [{'vulnerable': True, 'criteria': 'cpe:2.3:a:openresty:openresty:*:*:*:*:*:*:*:*', 'versionEndExcluding': '1.13.6.1', 'matchCriteriaId': 'A003256D-C746-
467A-9542-885CF4047996'}]}]
```

Figure 12: **Searching for CVE**

3 Conclusion

So RecoNess is created to simplify and improve efficiency of an attack for pentester or redteamer. RecoNess consists of tools use for different kind of purposes such as FFUF (Subdomain Scan), Dirsearch (Directory Scan), Nmap (Port Scan), Arjun (Parameters Scan), Whatweb (Technologies Scan) and CVE Search (CVE Scan).