# **Welcome to API Endpoint Discovery!**

**Remember to use python3 to run this file along side kali linux.**
List of tools to download:
- Subfinder: https://github.com/projectdiscovery/subfinder,
- Nuclei: https://github.com/projectdiscovery/nuclei,
- HTTPx: https://github.com/projectdiscovery/httpx,
- Feroxbuster: sudo apt-get install feroxbuster,
Python Libraries to Download or Check for Availibility:
- Subprocess
- Argparse
- datetime
- jinja2
- pdfkit
To download python libraries you can use the pip3 install command in command line.
Features
To run it, run the "apiDiscovery.py" file using python3 e.g. python3 apiDiscovery.py
There are 3 options at the moment.
1) t: to use the tools for scanning
2) -h: to bring up the help page
3) q: to quit the program
How to run:
python3 apiDiscovery.py [url to use e.g. google.com,twitter.com,thedogapi.com,megacorpone.com]

[choice: t,q,-h]

e.g. python3 apiDiscovery.py thedogapi.com t (to scan thedogapi.com and to use the tools for scanning the uri

\*\*\*\*Note: do not need to use any subdomains like www.xxx.com, https://api.xxx.com etc\*\*\*\*

## Step 1: Input your command into the command line:

```
root@kali-linux:/media/sf_Downloads/apiDiscoveryV1.4/apiDiscoveryV1.4# sudo pyth
on3 apiDiscovery.py thedogapi.com t
```

It will then proceed to check your system for the availability of the files

## Step 2: It will confirm the tools that you are going to run. (Consent)

```
root@kali-linux:/media/sf_Downloads/apiDiscoveryV1.4/apiDiscoveryV1.4

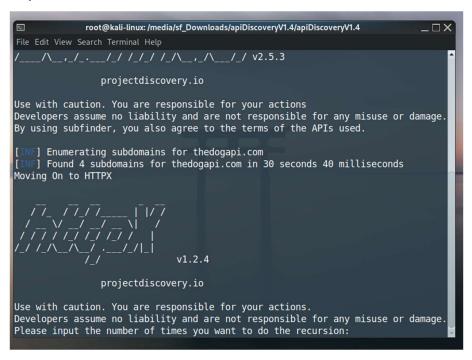
File Edit View Search Terminal Help

root@kali-linux:/media/sf_Downloads/apiDiscoveryV1.4/apiDiscoveryV1.4# sudo pyth
on3 apiDiscovery.py thedogapi.com t
Nuclei is Installed in your system.
Subfinder is installed in your system.
Feroxbuster is installed in your system.
GoLang is installed in your system.

### Error whilst finding httpx in your system. Installing HTTPX ###
You chose to use the tools!
Now Running Subfinder --> HTTPX --> FeroxBuster --> Nuclei!!
Continue?(Yes [y] or No [n]) :
```

- Insert Y for yes or N for no

## Step 3: Let it scan



Step 4: Input the number of times you want it to recurse.

Step 5: Input the wordlist you want to use.

```
/////_/\_/\_/\_/\_/\_/\_/\_/\_\\\

projectdiscovery.io

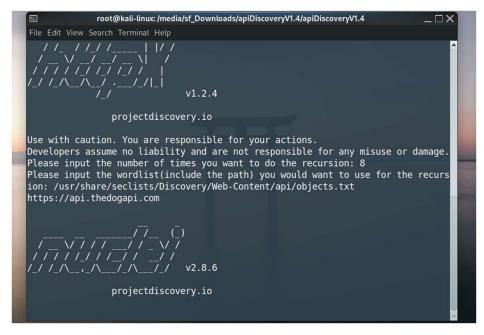
Use with caution. You are responsible for your actions.

Developers assume no liability and are not responsible for any misuse or damage.

Please input the number of times you want to do the recursion: 8

Please input the wordlist(include the path) you would want to use for the recursion: /usr/share/seclists/Discovery/Web-Content/api/objects.txt
```

Step 6: Let it scan!



Step 7: insert your whitelisted sites (in a readable text file with nextline inputs for new links See Appendix 1.0 for example) if needed. If not press enter

```
root@kali-linux:/media/sf_Downloads/apiDiscoveryV1.4/apiDiscoveryV1.4

File Edit View Search Terminal Help

please input your text file path for whitelisted sites:

nentsFinished Scanning

loads root@kali-linux:/media/sf_Downloads/apiDiscoveryV1.4/apiDiscoveryV1.4#

sc-htt vapid apised and vapid 1671427365 state

ei-te

sali-

# sudo pip3 install pdfkit
```

Step 8: Scan will be finished and a pdf will be outputted into the main directory.

```
root@kali-linux: /media/sf_Downloads/apiDiscoveryV1.4/apiDiscoveryV1.4
File Edit View Search Terminal Help
Please input your text file path for whitelisted sites:
inished Scanning
     ali-linux:/media/sf Downloads/apiDiscoveryV1.4/apiDiscoveryV1.4# ls
apiDiscovery.py
dependancyChecker.sh
ferox-https thedogapi com-1676008428.state
PDFCSV
README.txt
sonar-project properties
thedogapi.com02-Feb-2023 102449.pdf'
thedogapi.com26-Jan-2023 152500.pdf'
thedogapi.com30-Jan-2023 161919.pdf'
whitelist.txt
 oot@kali-linux:/media/sf Downloads/apiDiscoveryV1.4/apiDiscoveryV1.4#
```



# thedogapi.com Vulnerability Report

#### **Exposed SubDomains**

thedogapi.com www.thedogapi.com cdn2.thedogapi.com api.thedogapi.com

#### Exposed Ports & IP Addresses

```
\label{lem:https://api.thedogapi.com['[43]', '[application/json]', '[2404:6800:4003:c04::79]'] $$ https://api.thedogapi.com['[43]', '[application/json]', '[172.253.118.121]'] $$ https://www.thedogapi.com['[3137]', '[text/html]', '[2606:4700:3037::ac43:a782]'] $$ https://www.thedogapi.com['[3137]', '[text/html]', '[172.67.167.130]'] $$ https://www.thedogapi.com['[3137]', '[text/html]', '[2606:4700:3036::6815:5206]'] $$ https://thedogapi.com['[3137]', '[text/html]', '[104.21.82.6]'] $$ https://thedogapi.com['[3137]', '[text/html]', '[172.67.167.130]'] $$ https://thedogapi.com['[3137]', '[text/html]', '[104.21.82.6]'] $$ https://thedogapi.com['[3137]', '[text/html]', '[104.21.82.6]'] $$ https://thedogapi.com['[3137]', '[text/html]', '[2606:4700:3037::ac43:a782]'] $$
```

# **Exposed Endpoints**

https://thedogapi.com/favicon.ico/ https://thedogapi.com/index/ => / https://www.thedogapi.com/favicon.ico/ https://api.thedogapi.com/ https://api.thedogapi.com/v1/

#### Nuclei Vulnerabilities

[dns-waf-detect:cloudflare] [dns] [info] www.thedogapi.com [google-frontend-httpserver] [http] [info] https://api.thedogapi.com/

D l.	I = =
Prob	iems

If you run into any problems email me at aureliusng@bdo.com.sg the issues along with the screenshot of said issue.

## Thanks!

------ Things to Note ------

- 1) Please run this with escalated privileges.
  - 2) Make sure the app is able to open the text files you have specified.
  - 3) Wordlists or text files' names are case sensitive.
  - 4) Must have stable internet.
  - 5) Download all libraries from python and linux prior.
- 6) App should be run in kali linux.

# **Appendix**

Item 1.0

https://api.thedogapi.com/v1/categories/ https://api.thedogapi.com/v1/facts/