Report2,3

Crawling :

1. Waybackurls

Accept line-delimited domains on stdin, fetch known URLs from the Wayback Machine for \*.domain and output them on stdout.

Install:

1. Install go
2. go/bin
3. go install [github.com/tomnomnom/waybackurls@latest](mailto:github.com/tomnomnom/waybackurls@latest)

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Katana

katana requires Go 1.18 to install successfully. To install, just run the below command or download pre-compiled binary from release page.

Install:

1. Go/bin
2. go install [github.com/projectdiscovery/katana/cmd/katana@latest](mailto:github.com/projectdiscovery/katana/cmd/katana@latest)

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. GAU

getallurls (gau) fetches known URLs from AlienVault's Open Threat Exchange, the Wayback Machine, Common Crawl, and URLScan for any given domain. Inspired by Tomnomnom's waybackurls.

Usage:

gau example.com google.com

A screen shot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

4-gospider

**Painless integrate Gospider into your recon workflow?**

[](https://raw.githubusercontent.com/osmedeus/assets/main/logo-transparent.png)

this project was part of Osmedeus Engine. Check out how it was integrated at [@OsmedeusEngine](https://twitter.com/OsmedeusEngine)

install:

1-go/bin

2-go install github.com/jaeles-project/gospider@latest

**Features**

* Fast web crawling
* Brute force and parse sitemap.xml
* Parse robots.txt
* Generate and verify link from JavaScript files
* Link Finder

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

5-hakrawler

Fast golang web crawler for gathering URLs and JavaScript file locations. This is basically a simple implementation of the awesome Gocolly library.

Usage:

echo https://google.com | hakrawler

cat urls.txt | hakrawler

A screenshot of a computer

Description automatically generated

6- linkfinder

LinkFinder is a python script written to discover endpoints and their parameters in JavaScript files. This way penetration testers and bug hunters are able to gather new, hidden endpoints on the websites they are testing. Resulting in new testing ground, possibility containing new vulnerabilities. It does so by using jsbeautifier for python in combination with a fairly large regular expression. The regular expressions consists of four small regular expressions. These are responsible for finding:

Install:

git clone <https://github.com/GerbenJavado/LinkFinder.git>

pip3 install -r requirements.txt

cd LinkFinder

A screenshot of a computer

Description automatically generatedA screenshot of a computer program

Description automatically generatedA screenshot of a computer

Description automatically generated

7-paramspider

paramspider allows you to fetch URLs related to any domain or a list of domains from Wayback achives. It filters out "boring" URLs, allowing you to focus on the ones that matter the most.

Install:

git clone https://github.com/devanshbatham/paramspider

cd paramspider

pip install .

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer program

Description automatically generated