



# Waybackurls – Hacker Tools: Time-traveling for bounties ☐☐

BY ANNA HAMMOND · SEPTEMBER 24, 2021 · LAST UPDATED ON MARCH 6, 2025

The past can tell stories, show things that should've never been uncovered and today we will be looking at that past. We can go hunt for subdomains, secret endpoints, tokens, and secrets, all with the help of Waybackurls.

Wayback Machine Logo

## ☐☐ What is Waybackurls?

Waybackurls by [@TomNomNom](#) is a small utility written in Go that will fetch known URLs from the Wayback Machine and Common Crawl. (For more information on these services, read the remainder of the article!)

It is a very small utility that does what it was designed for and does it well.

## What can you find with Waybackurls?

- Subdomains

This is a great way to passively and incredibly quickly gather subdomains that have actually been used in the past (and are potentially still in use or outdated today). In fact, most popular subdomain enumeration tools such as [Amass](#) also search through the Wayback Machine for subdomains.

- Endpoints

Perhaps this one is a bit too obvious but yes, this will give you a large list of endpoints that can be tested. Additionally, this scan is way faster than brute force content enumeration tools such as [Gobuster](#).

- Tokens & secrets

People have used this technique in the past to find a valid session or API keys and secrets in the GET parameters for requests found by Waybackurls. An example is [this blog article](#).

- IDs and secret files

Ever come across applications where you upload a file, perhaps containing sensitive data, and it gets stored in `/files/932c847ab1288734dfe234234` ? Did you wonder if you could find more files there? Perhaps Waybackurls will show you another one and help you disclose information!

## ☐☐ Our first run!

Check out the video below for an example of how you can use Waybackurls!

# ☐☐ Setting up Waybackurls

Installing Waybackurls is as simple as counting to ten!

1. Download the appropriate release from the [releases on Github](#).
2. Untar the file through `tar -xf file`
3. Enjoy the `waybackurls` binary

# ☐☐ Services making Waybackurls possible

As discussed earlier, this tool uses the Wayback Machine and Common Crawl to search for results. Let's take a very quick look at these services.

- [Wayback Machine](#)  
[This service](#) was created when the internet was still making its first baby steps. It has archived over 614 billion web pages over the last decades and these have been either manually archived or crawled.
- [Common Crawl](#)  
[Common Crawl](#) is another project that crawls millions of sites to keep a public record of the results. You can query these, which is what the tool does.

For more information, be sure to check out their websites!

## Conclusion

Waybackurls is a tiny, yet helpful utility to help you uncover the past. Start using it today and let's get some easy wins!

If you would like to recommend a tool for us to cover next week, then be sure to let us know down below. Also be sure to check out [all the previous Hacker Tools articles](#), such as [the last one on Dalfox](#).

---

Did you know that there is a video accompanying this article? Check out [the playlist](#)!

REQUEST A DEMO

[intigrity.com/demo](https://intigrity.com/demo)

VISIT THE WEBSITE

[intigrity.com](https://intigrity.com)

GET IN TOUCH

[hello@intigrity.com](mailto:hello@intigrity.com)