



CRLFuzz – Hacker Tools: Injecting CRLF for bounties ☐☐

BY ANNA HAMMOND · OCTOBER 5, 2021 · LAST UPDATED ON MARCH 6, 2025

A CRLF injection is the injection of newlines in places where the server doesn't expect newlines. This can cause a plethora of vulnerabilities including XSS, session fixation, cookie injection, open redirect, and much more! What are we waiting for? Let's check out CRLFuzz, the tool that can help you!



CRLFuzz ASCII art

☐☐ What is CRLFuzz?

CRLFuzz is a tool written in Go by [@dwwiswant0](#) that helps you find CRLF injections with ease!

It takes a list of URLs and will attempt to inject a header using a list of payloads. If it detects that a header was successfully injected, you'll be alerted of it. It's as easy as that.

☐☐ Our first run!

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

☐☐ Installing CRLFuzz

Want to install CRLFuzz? Well, just download the [GitHub releases](#), untar and done!

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

Command line options

What to fuzz?

- `-u` or `-url` can be used to define a URL to fuzz.
- `-l` or `-list` can be used to specify a file with URLs to fuzz.

What kind of request are we sending?

- **-X** or **-method** can be used to specify the request method to be used. This option defaults to GET.
- **-d** or **-data** can be used to define additional request data.
- **-H** or **-header** can be used to set a custom header to pass to the target.

Outputting what?

- **-o** or **-output** can be used to save results to a file.
- **-v** or **-verbose** can be used to show more information.
- **-s** or **-silent** can be used to not output anything.

Other useful options?

- **-c** or **-concurrent** can be used to set how many concurrent connections will be made. The default is 25.
- **-x** or **-proxy** can be used to specify a proxy.

Conclusion

CRLFuzz is a tiny, yet helpful tool to find those injection points for your secretive CRLFs. Start using it today and let's get some bounties!

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 Waybackurls](#).

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

REQUEST A DEMO

intigrity.com/demo

VISIT THE WEBSITE

intigrity.com

GET IN TOUCH

hello@intigrity.com