

Fuzz Faster U Fool - v2.1.0

HTTP OPTIONS:

-H Header `"Name: Value"`, separated by colon. Multiple **-H** flags are accepted.

-X HTTP method to use

-b Cookie data `"NAME1=VALUE1; NAME2=VALUE2"` for copy as curl functionality.

-cc Client cert for authentication. Client key needs to be defined as well for this to work

-ck Client key for authentication. Client certificate needs to be defined as well for this to work

-d POST data

-http2 Use HTTP2 protocol (default: false)

-ignore-body
Do not fetch the response content. (default: false)

-r Follow redirects (default: false)

-raw Do not encode URI (default: false)

-recursion
Scan recursively. Only FUZZ keyword is supported, and URL (**-u**) has to end in it. (default: false)

-recursion-depth
Maximum recursion depth. (default: 0)

-recursion-strategy Recursion strategy:
"default" for a redirect based, and "greedy" to recurse on all matches (default: default)

-replay-proxy
Replay matched requests using this proxy.

-sni Target TLS SNI, does not support FUZZ keyword

-timeout HTTP request timeout in seconds. (default: 10)

-u Target URL

-x Proxy URL (SOCKS5 or HTTP). For example:
http://127.0.0.1:8080 or socks5://127.0.0.1:8080

GENERAL OPTIONS:

-V Show version information. (default: false)

-ac Automatically calibrate filtering options (default: false)

-acc Custom auto-calibration string. Can be used multiple times.
Implies **-ac**

-ach Per host autocalibration (default: false)

-ack Autocalibration keyword (default: FUZZ)

-acs Custom auto-calibration strategies. Can be used multiple times.
Implies **-ac**

-c Colorize output. (default: false)

-config Load configuration from a file

-json JSON output, printing newline-delimited JSON records (default: false)

-maxtime Maximum running time in seconds for entire process. (default: 0)

-maxtime-job
Maximum running time in seconds per job. (default: 0)

-noninteractive
Disable the interactive console functionality (default: false)

-p Seconds of `delay` between requests, or a range of random delay. For example "0.1" or "0.1-2.0"

-rate Rate of requests per second (default: 0)

-s Do not print additional information (silent mode) (default: false)

-sa Stop on all error cases. Implies **-sf** and **-se**. (default: false)

-scraperfile
Custom scraper file path

-scrapers Active scraper groups (default: all)

-se Stop on spurious errors (default: false)

-search Search for a FFUFHASH payload from ffuf history

-sf Stop when > 95% of responses return 403 Forbidden (default: false)

-t Number of concurrent threads. (default: 40)

-v Verbose output, printing full URL and redirect location (if any) with the results. (default: false)

MATCHER OPTIONS:

-mc Match HTTP status codes, or "all" for everything. (default: 200-299,301,302,307,401,403,405,500)

-ml Match amount of lines in response

-mmode Matcher set operator. Either of: and, or (default: or)

-mr Match regexp

-ms Match HTTP response size

-mt Match how many milliseconds to the first response byte, either greater or less than. EG: >100 or <100

-mw Match amount of words in response

FILTER OPTIONS:

-fc Filter HTTP status codes from response. Comma separated list of codes and ranges

-fl Filter by amount of lines in response. Comma separated list of line counts and ranges

-fmode Filter set operator. Either of: and, or (default: or)

-fr Filter regexp

-fs Filter HTTP response size. Comma separated list of sizes and ranges

-ft Filter by number of milliseconds to the first response byte, either greater or less than. EG: >100 or <100

-fw Filter by amount of words in response. Comma separated list of word counts and ranges

INPUT OPTIONS:

-D DirSearch wordlist compatibility mode. Used in conjunction with **-e** flag. (default: false)

-e Comma separated list of extensions. Extends FUZZ keyword.

-enc Encoders for keywords, eg. 'FUZZ:urlencode b64encode'

-ic Ignore wordlist comments (default: false)

-input-cmd Command producing the input. **--input-num** is required when using this input method. Overrides **-w**.

-input-num Number of inputs to test. Used in conjunction with **--input-cmd**. (default: 100)

-input-shell Shell to be used for running command

-mode Multi-wordlist operation mode. Available modes: clusterbomb, pitchfork, sniper (default: clusterbomb)

-request File containing the raw http request

-request-proto Protocol to use along with raw request (default: https)

-w Wordlist file path and (optional) keyword separated by colon. eg. '/path/to/wordlist:KEYWORD'

OUTPUT OPTIONS:

-debug-log Write all of the internal logging to the specified file.

-o Write output to file

-od Directory path to store matched results to.

-of Output file format. Available formats: json, ejson, html, md, csv, ecsv (or, 'all' for all formats) (default: json)

-or Don't create the output file if we don't have results (default: false)

EXAMPLE USAGE:

Fuzz file paths from wordlist.txt, match all responses but filter out those with content-size 42.

Colored, verbose output.

```
ffuf -w wordlist.txt -u https://example.org/FUZZ -mc all -fs 42 -c -v
```

Fuzz Host-header, match HTTP 200 responses.

```
ffuf -w hosts.txt -u https://example.org/ -H "Host: FUZZ" -mc 200
```

Fuzz POST JSON data. Match all responses not containing text "error".

```
ffuf -w entries.txt -u https://example.org/ -X POST -H "Content-Type: application/json" \
```

```
-d '{"name": "FUZZ", "anotherkey": "anothervalue"}' -fr "error"
```

Fuzz multiple locations. Match only responses reflecting the value of "VAL" keyword. Colored.

```
ffuf -w params.txt:PARAM -w values.txt:VAL -u https://example.org/?PARAM=VAL -mr "VAL" -c
```

More information and examples: <https://github.com/ffuf/ffuf>