



## Gobuster Cheatsheet



### Gobuster Cheatsheet

Gobuster is a tool for brute forcing URIs (Files and Directories) and DNS subdomains.

The help section can provide options for Gobuster.

```
“ gobuster -h”
```

```
root@kali:~# gobuster -h
Usage of gobuster:
  -P string
```

```
        Password for Basic Auth (dir mode only)
-U string
    Username for Basic Auth (dir mode only)
-a string
    Set the User-Agent string (dir mode only)
-c string
    Cookies to use for the requests (dir mode only)
-cn
    Show CNAME records (dns mode only, cannot be used with '-i' option)
-e
    Expanded mode, print full URLs
-f
    Append a forward-slash to each directory request (dir mode only)
-fw
    Force continued operation when wildcard found
-i
    Show IP addresses (dns mode only)
-k
    Skip SSL certificate verification
-l
    Include the length of the body in the output (dir mode only)
-m string
    Directory/File mode (dir) or DNS mode (dns) (default "dir")
-n
    Don't print status codes
-np
    Don't display progress
-o string
    Output file to write results to (defaults to stdout)
-p string
    Proxy to use for requests [http(s)://host:port] (dir mode only)
-q
    Don't print the banner and other noise
-r
    Follow redirects
-s string
    Positive status codes (dir mode only) (default "200,204,301,302,307,403")
-t int
    Number of concurrent threads (default 10)
-to duration
    HTTP Timeout in seconds (dir mode only) (default 10s)
-u string
    The target URL or Domain
-v
    Verbose output (errors)
-w string
    Path to the wordlist
```

```
-x string  
    File extension(s) to search for (dir mode only)
```

## Common Command line options

- -fw – force processing of a domain with wildcard results.
- -np – hide the progress output.
- -m – which mode to use, either dir or dns (default: dir).
- -q – disables banner/underline output.
- -t
- – number of threads to run (default: 10).
- -u – full URL (including scheme), or base domain name.
- -v – verbose output (show all results).
- -w – path to the wordlist used for brute forcing (use - for stdin).

### Command line options for dns mode

- -cn – show CNAME records (cannot be used with '-i' option).
- -i – show all IP addresses for the result.

### Command line options for dir mode

- -a <user agent string> – specify a user agent string to send in the request header.
- -c <http cookies> – use this to specify any cookies that you might need (simulating auth).
- -e – specify extended mode that renders the full URL.
- -f – append / for directory brute forces.
- -k – Skip verification of SSL certificates.
- -l – show the length of the response.
- -n – “no status” mode, disables the output of the result’s status code.
- -o <file> – specify a file name to write the output to.
- -p <proxy url> – specify a proxy to use for all requests (scheme must match the URL scheme).
- -r – follow redirects.

- **-s <status codes>** – comma-separated set of the list of status codes to be deemed a “positive” (default: 200,204,301,302,307).
- **-x <extensions>** – list of extensions to check for, if any.
- **-P <password>** – HTTP Authorization password (Basic Auth only, prompted if missing).
- **-U <username>** – HTTP Authorization username (Basic Auth only).
- **-to <timeout>** – HTTP timeout. Examples: 10s, 100ms, 1m (default: 10s).

## Wordlist Usage

“ gobuster -w <wordlist.txt> ”

```
root@kali:~# gobuster -u http://192.168.2.62/dvwa -w /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-small.txt -t 40 -x .php,.txt,.html
=====
Gobuster v2.0.0          OJ Reeves (@TheColonial)
=====
[+] Mode      : dir
[+] Url/Domain : http://192.168.2.62/dvwa/
[+] Threads   : 40
[+] Wordlist  : /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-small.txt
[+] Status codes: 200,204,301,302,307,403
[+] Extensions: php,txt,html
[+] Timeout   : 10s
=====
2018/11/19 01:50:12 Starting gobuster
=====
/index (Status: 302)
/index.php (Status: 302)
/security (Status: 302)
/security.php (Status: 302)
/docs (Status: 301)
/login (Status: 200)
/login.php (Status: 200)
/about (Status: 302)
/about.php (Status: 302)
/external (Status: 301)
/logout (Status: 302)
/logout.php (Status: 302)
/config (Status: 301)
/robots (Status: 200)
/robots.txt (Status: 200)
/favicon (Status: 200)
/setup (Status: 200)
/setup.php (Status: 200)
/vulnerabilities (Status: 301)
/instructions (Status: 302)
/instructions.php (Status: 302)
```

The wordlist switch specifies a wordlist that can be used for brute forcing directories.

## URL Usage

“ gobuster -u <url>”

```
root@kali:~# gobuster -u http://192.168.2.62/dvwa -w /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-small.txt -t 40 -x .php,.txt,.html
=====
Gobuster v2.0.0          OJ Reeves (@TheColonial)
=====
[+] Mode     : dir
[+] Url/Domain  : http://192.168.2.62/dvwa/
[+] Threads   : 40
[+] Wordlist  : /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-small.txt
[+] Status codes: 200,204,301,302,307,403
[+] Extensions: php,txt,html
[+] Timeout    : 10s
=====
2018/11/19 01:50:12 Starting gobuster
=====
/index (Status: 302)
/index.php (Status: 302)
/security (Status: 302)
/security.php (Status: 302)
/docs (Status: 301)
/login (Status: 200)
/login.php (Status: 200)
/about (Status: 302)
/about.php (Status: 302)
/external (Status: 301)
/logout (Status: 302)
/logout.php (Status: 302)
/config (Status: 301)
/robots (Status: 200)
/robots.txt (Status: 200)
/favicon (Status: 200)
/setup (Status: 200)
/setup.php (Status: 200)
/vulnerabilities (Status: 301)
/instructions (Status: 302)
/instructions.php (Status: 302)
```

The URL switch specifies the website name that will be scanned.

## Thread Usage

“ gobuster -t <Num>”

```
root@kali:~# gobuster -u http://192.168.2.62/dvwa -w /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-small.txt -t 40 -x .php,.txt,.html
=====
Gobuster v2.0.0          OJ Reeves (@TheColonial)
=====
[+] Mode      : dir
[+] Url/Domain : http://192.168.2.62/dvwa/
[+] Threads   : 40
[+] Wordlist  : /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-small.txt
[+] Status codes: 200,204,301,302,307,403
[+] Extensions: php,txt,html
[+] Timeout   : 10s
=====
2018/11/19 01:50:12 Starting gobuster
=====
/index (Status: 302)
/index.php (Status: 302)
/security (Status: 302)
/security.php (Status: 302)
/docs (Status: 301)
/login (Status: 200)
/login.php (Status: 200)
/about (Status: 302)
/about.php (Status: 302)
/external (Status: 301)
/logout (Status: 302)
/logout.php (Status: 302)
/config (Status: 301)
/robots (Status: 200)
/robots.txt (Status: 200)
/favicon (Status: 200)
/setup (Status: 200)
/setup.php (Status: 200)
/vulnerabilities (Status: 301)
/instructions (Status: 302)
/instructions.php (Status: 302)
```

The thread switch specifies the number of concurrent threads that will run at the same time.

## Extension Usage

“ gobuster -x <ext>”

```
root@kali:~# gobuster -u http://192.168.2.62/dvwa -w /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-small.txt -t 40 -x .php,.txt,.html
=====
Gobuster v2.0.0          OJ Reeves (@TheColonial)
=====
[+] Mode      : dir
[+] Url/Domain : http://192.168.2.62/dvwa/
[+] Threads   : 40
[+] Wordlist  : /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-small.txt
[+] Status codes: 200,204,301,302,307,403
[+] Extensions: php,txt,html
[+] Timeout   : 10s
=====
2018/11/19 01:50:12 Starting gobuster
=====
/index (Status: 302)
/index.php (Status: 302)
/security (Status: 302)
/security.php (Status: 302)
/docs (Status: 301)
/login (Status: 200)
/login.php (Status: 200)
/about (Status: 302)
/about.php (Status: 302)
/external (Status: 301)
/logout (Status: 302)
/logout.php (Status: 302)
/config (Status: 301)
/robots (Status: 200)
/robots.txt (Status: 200)
/favicon (Status: 200)
/setup (Status: 200)
/setup.php (Status: 200)
/vulnerabilities (Status: 301)
/instructions (Status: 302)
/instructions.php (Status: 302)
```

The extension switch specifies the file extensions. Multiple extensions may be listed separated by commas.

## String Usage

“ gobuster -s “<string>””

```
root@kali:~# gobuster -u http://192.168.2.62/dvwa -w /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-small.txt -t 40 -x .php,.txt,.html -s "200"
=====
Gobuster v2.0.0          OJ Reeves (@TheColonial)
=====
[+] Mode     : dir
[+] Url/Domain : http://192.168.2.62/dvwa/
[+] Threads   : 40
[+] Wordlist  : /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-small.txt
[+] Status codes : 200
[+] Extensions : php,txt,html
[+] Timeout    : 10s
=====
2018/11/19 02:09:04 Starting gobuster
=====
/login (Status: 200)
/login.php (Status: 200)
/favicon (Status: 200)
/robots (Status: 200)
/robots.txt (Status: 200)
/setup (Status: 200)
/setup.php (Status: 200)
Progress: 39838 / 326576 (12.20%)^C
```

The string switch specifies the results that are being displayed.

## Expanded Mode Usage

“ gobuster -e”

```
root@kali:~# gobuster -e -u http://192.168.2.62/dvwa -w /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-small.txt -t 40 -x .php,.txt,.html -s "200"
=====
Gobuster v2.0.0          OJ Reeves (@TheColonial)
=====
[+] Mode     : dir
[+] Url/Domain : http://192.168.2.62/dvwa/
[+] Threads   : 40
[+] Wordlist  : /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-small.txt
[+] Status codes : 200
[+] Extensions : php,txt,html
[+] Expanded   : true
[+] Timeout    : 10s
=====
2018/11/19 02:30:23 Starting gobuster
=====
http://192.168.2.62/dvwa/login (Status: 200)
http://192.168.2.62/dvwa/login.php (Status: 200)
http://192.168.2.62/dvwa/favicon (Status: 200)
http://192.168.2.62/dvwa/robots (Status: 200)
http://192.168.2.62/dvwa/robots.txt (Status: 200)
http://192.168.2.62/dvwa/setup (Status: 200)
http://192.168.2.62/dvwa/setup.php (Status: 200)
```

The expanded mode switch shows the full URL path in the results.

## No Status Usage

“ gobuster -n”

```
root@kali:~# gobuster -u http://192.168.2.62/dvwa -w /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-small.txt -x .php,.txt,.html -s "200" -n
=====
Gobuster v2.0.0          OJ Reeves (@TheColonial)
=====
[+] Mode      : dir
[+] Url/Domain  : http://192.168.2.62/dvwa/
[+] Threads   : 10
[+] Wordlist  : /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-small.txt
[+] Status codes: 200
[+] Extensions: php,txt,html
[+] No status  : true
[+] Timeout    : 10s
=====
2018/11/19 02:39:26 Starting gobuster
=====
/login
/login.php
/favicon
/robots
/robots.txt
/setup
/setup.php
```

The no status mode will exclude the status codes in the results.

## Verbose Mode

“ gobuster -v”

```
root@kali:~# gobuster -u http://192.168.2.62/dvwa -w /usr/share/dirb/wordlists/common.txt -v
=====
Gobuster v2.0.0          OJ Reeves (@TheColonial)
=====
[+] Mode      : dir
[+] Url/Domain  : http://192.168.2.62/dvwa/
[+] Threads   : 10
[+] Wordlist  : /usr/share/dirb/wordlists/common.txt
[+] Threads   : 10
[+] Timeout    : 10s
```

```
[+] Status codes : 200,204,301,302,307,403
[+] Verbose      : true
[+] Timeout      : 10s
=====
2018/11/19 02:46:36 Starting gobuster
=====
Missed: /.bash_history (Status: 404)
Found: /.hta (Status: 403)
Missed: /.config (Status: 404)
Missed: /.bashrc (Status: 404)
Found: /.htaccess (Status: 403)
Missed: /.cache (Status: 404)
Missed: /.git/HEAD (Status: 404)
Missed: /.forward (Status: 404)
Missed: /.listing (Status: 404)
Missed: /.cvs (Status: 404)
Missed: /.cvignore (Status: 404)
Missed: /.mysql_history (Status: 404)
Missed: /.profile (Status: 404)
Missed: /.listings (Status: 404)
Missed: /.passwd (Status: 404)
Missed: /.sh_history (Status: 404)
Missed: /.rhosts (Status: 404)
Missed: /.ssh (Status: 404)
Found: /.htpasswd (Status: 403)
Missed: /.perf (Status: 404)
Missed: /.subversion (Status: 404)
Missed: /.svn (Status: 404)
Missed: /.history (Status: 404)
Missed: /.svn/entries (Status: 404)
Missed: /.swf (Status: 404)
Missed: /.web (Status: 404)
Missed: /@ (Status: 404)
Missed: /_ (Status: 404)
Missed: /_adm (Status: 404)
Missed: /_admin (Status: 404)
Missed: /_ajax (Status: 404)
Missed: /_archive (Status: 404)
Missed: /_assets (Status: 404)
Missed: /_backup (Status: 404)
```

The verbose mode will increase the logging level of the search results.

# User Agent

“ gobuster -a <useragent>”

```
root@kali:~# gobuster -u http://192.168.2.62/dvwa -w /usr/share/dirb/wordlists/common.txt -a CustomAgent
=====
Gobuster v2.0.0          OJ Reeves (@TheColonial)
=====
[+] Mode      : dir
[+] Url/Domain  : http://192.168.2.62/dvwa/
[+] Threads   : 10
[+] Wordlist   : /usr/share/dirb/wordlists/common.txt
[+] Status codes: 200,204,301,302,307,403
[+] User Agent  : CustomAgent
[+] Timeout    : 10s
=====
2018/11/19 03:12:45 Starting gobuster
=====
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/about (Status: 302)
/config (Status: 301)
/docs (Status: 301)
/external (Status: 301)
/favicon.ico (Status: 200)
/index.php (Status: 302)
/index (Status: 302)
/instructions (Status: 302)
/logout (Status: 302)
/login (Status: 200)
/php.ini (Status: 200)
/phpinfo.php (Status: 302)
/phpinfo (Status: 302)
/README (Status: 200)
```

The user agent options give the ability to change the appearance of the requests for bypassing filters.

## Export Option

“ gobuster -o <filename>”

```
root@kali:~# gobuster -u http://192.168.2.62/dvwa -w /usr/share/dirb/wordlists/common.txt -o output.txt
=====
Gobuster v2.0.0          OJ Reeves (@TheColonial)
=====
[+] Mode      : dir
[+] Url/Domain  : http://192.168.2.62/dvwa/
[+] Threads   : 10
[+] Wordlist   : /usr/share/dirb/wordlists/common.txt
[+] Status codes : 200,204,301,302,307,403
[+] Timeout    : 10s
=====
2018/11/19 03:19:08 Starting gobuster
=====
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/.hta (Status: 403)
/about (Status: 302)
/config (Status: 301)
/docs (Status: 301)
/external (Status: 301)
/favicon.ico (Status: 200)
/index.php (Status: 302)
/index (Status: 302)
/instructions (Status: 302)
/logout (Status: 302)
/login (Status: 200)
/php.ini (Status: 200)
/phpinfo.php (Status: 302)
/phpinfo (Status: 302)
/README (Status: 200)
/robots (Status: 200)
/robots.txt (Status: 200)
/security (Status: 302)
/setup (Status: 200)
=====
2018/11/19 03:19:10 Finished
=====
root@kali:~# cat output.txt
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
```

```
/.mcpasswd (Status: 403)
/.hta (Status: 403)
/about (Status: 302)
/config (Status: 301)
/docs (Status: 301)
/external (Status: 301)
```

The output option saves the results to file in text format.

 *Previous post*

[Hack The Box: Brainf#@k](#)

*Next post* 

[Hack The Box: Sense](#)