

# A Detailed Guide on **Feroxbuster**

Feroxbuster is a robust tool designed to identify directories and files on web servers using brute-force techniques. It is frequently utilized in penetration testing and security evaluations to detect concealed paths and resources. Here we are going to discuss about various tasks which we can perform using Feroxbuster.

## Table of Contents

- **Lab setup**
- **Installation**
- **Default mode**
- **Redirects**
- **Extensions**
- **Result output**
- **User agent**
- **Filter status code**
- **Quiet mode**
- **Controlling threads**
- **Custom wordlist**
- **Disable recursion**
- **Limit recursion depth**
- **Force Recursion**
- **Filter by character size**
- **Filter by number of words**
- **Filter by number of lines**
- **Filter by status code using deny list**
- **Filter by status code using allow list**
- **Generating random User-Agent**
- **HTTP methods**
- **Custom headers**
- **Cookies**
- **Adding slash**
- **Capturing requests in Burp**
- **Read target from list**
- **Resume from last state**

- Follow redirect
- Timeout
- Comparasion between Feroxbuster and other tools
- Conclusion

## Lab setup

Target Machine: 192.168.1.4

Attacker Machine: 192.168.1.31 (Kali Linux)

After setting up a web server in the target machine, we can proceed with the enumeration in the kali linux after installing Feroxbuster.

## Installation

To install the Feroxbuster in kali linux, we can use the following command:

```
apt install feroxbuster
```

```
└─(root㉿kali)-[~]
└─# apt install feroxbuster ←
feroxbuster is already the newest version (2.10).
The following packages were automatically installed:
  libabsl20220623  libboost-iostreams1.74.0  lib
  libadwaita-1-0    libboost-thread1.74.0      lib
  libaiodns          libboost1.83-dev        lib
```

## Default mode

Once we are done with the installation, we can proceed with the enumeration part. To perform a default directory brute force, we can use the following the command:

```
feroxbuster -u http://192.168.1.4
```

```
—(root㉿kali)-[~]
# feroxbuster -u http://192.168.1.4 ↵

[+] [+] [ ]) [ ]) | / \ ,   [ ]) X\ | | \ ) | —
by Ben "epi" Risher ☺ ver: 2.10.4

① Target Url           http://192.168.1.4
Threads                 50
② Wordlist               /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
③ Status Codes          All Status Codes!
Timeout (secs)          7
User-Agent              feroxbuster/2.10.4
Config File             /etc/feroxbuster/ferox-config.toml
④ Extract Links         true
⑤ HTTP methods           [GET]
⑥ Recursion Depth       4

Press [ENTER] to use the Scan Management Menu™

+03    GET    11l    32w      -c Auto-filtering found 404-like response and created new filt
+04    GET    9l     32w      -c Auto-filtering found 404-like response and created new filt
302    GET    0l     0w       0c http://192.168.1.4/ => login.php
301    GET    9l     28w     309c http://192.168.1.4/docs => http://192.168.1.4/docs/
301    GET    9l     28w     311c http://192.168.1.4/config => http://192.168.1.4/config/
200    GET    47l    282w    1859c http://192.168.1.4/config/config.inc.php.bak
301    GET    9l     28w     313c http://192.168.1.4/external => http://192.168.1.4/external/
301    GET    9l     28w     324c http://192.168.1.4/external/phpids/0.6 => http://192.168.1.4/external/phpids/0.6
200    GET    0l     0w       0c http://192.168.1.4/external/recaptcha/recaptchalib.php
+04    GET    9l     33w     289c http://192.168.1.4/external%20files
+01    GET    0l     0w       0c http://192.168.1.4/0/1.vhost
```

It can be seen from above that the wordlist used in default mode is the **raft-medium-directories.txt**.

To get a less verbose output, we can use the **--silent** flag to hide the non-essential data.

```
feroxbuster -u http://192.168.1.4 --silent
```

```
[root@kali]~# feroxbuster -u http://192.168.1.4 --silent ←  
  
http://192.168.1.4/  
http://192.168.1.4/docs  
http://192.168.1.4/config  
http://192.168.1.4/docs/pdf.html  
http://192.168.1.4/config/config.inc.php.dist  
http://192.168.1.4/config/config.inc.php  
http://192.168.1.4/external  
http://192.168.1.4/external/recaptcha/recaptchalib.php  
http://192.168.1.4/Reports%20List  
http://192.168.1.4/docs/DVWA_v1.3.pdf  
http://192.168.1.4/Style%20Library  
http://192.168.1.4/config/config.inc.php.bak  
http://192.168.1.4/neuf%20giga%20photo  
http://192.168.1.4/external/phpids/0.6  
http://192.168.1.4/My%20Project  
http://192.168.1.4/Donate%20Cash  
http://192.168.1.4/Home%20Page  
http://192.168.1.4/Press%20Releases  
http://192.168.1.4/Site%20Map  
http://192.168.1.4/Gift%20Form  
http://192.168.1.4/Life%20Income%20Gift  
http://192.168.1.4/New%20Folder  
http://192.168.1.4/Site%20Assets  
http://192.168.1.4/What%20is%20New
```

## Redirects

In order to allow the Feroxbuster to continue the directory brute forcing on the redirected URL, we can use the **-r** or **--redirect** flag. For example if `http://192.168.1.4` redirects to `http://192.168.1.4/newpath`, Feroxbuster will follow this redirection and continue to scan `http://192.168.1.4/newpath` for directories and files.

```
feroxbuster -u http://192.168.1.4 -r
```

```
(root㉿kali)-[~]
# feroxbuster -u http://192.168.1.4 -r ←

[+] [+] [ ]) | \_,    [ ] ) ) / | [ ] | [ ]
by Ben "epi" Risher ↵ ver: 2.10.4

🕒 Target Url          http://192.168.1.4
🚀 Threads              50
📝 Wordlist             /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
🔥 Status Codes         All Status Codes!
⌚ Timeout (secs)       7
⚡ User-Agent            feroxbuster/2.10.4
📌 Config File          /etc/feroxbuster/ferox-config.toml
🌐 Extract Links        true
🚩 HTTP methods         [GET]
📍 Follow Redirects    true
🔃 Recursion Depth      4

※ Press [ENTER] to use the Scan Management Menu™

404   GET    9l    32w      -c Auto-filtering found 404-like response and created new
403   GET    11l   32w      -c Auto-filtering found 404-like response and created new
200   GET    47l   282w     1864c http://192.168.1.4/config/config.inc.php.dist
200   GET    47l   282w     1859c http://192.168.1.4/config/config.inc.php.bak
200   GET    0l    0w       0c http://192.168.1.4/config/config.inc.php
200   GET    1l    10w      105c http://192.168.1.4/docs/pdf.html
200   GET    59l   101w     842c http://192.168.1.4/dvwa/css/login.css
200   GET    39l   244w     16182c http://192.168.1.4/dvwa/images/login_logo.png
200   GET    0l    0w       0c http://192.168.1.4/external/recaptcha/recaptchalib.php
200   GET    165l  1234w    7639c http://192.168.1.4/external/phpids/0.6/LICENSE
200   GET    2922l 17217w   730335c http://192.168.1.4/docs/DVWA_v1.3.pdf
200   GET    17l   69w      1136c http://192.168.1.4/docs/
```

## Extensions

To perform brute-force for a particular type of file extension, the **-x** or **--extensions** flag can be used.

```
feroxbuster -u http://192.168.1.4 -x php,txt --silent
```

```
[root@kali:~]# feroxbuster -u http://192.168.1.4 -x php,txt --silent ←  
  
http://192.168.1.4/  
http://192.168.1.4/docs  
http://192.168.1.4/config  
http://192.168.1.4/config/config.inc.php.dist  
http://192.168.1.4/config/config.inc.php.bak  
http://192.168.1.4/dvwa/js/add_event_listeners.js  
http://192.168.1.4/dvwa/css/main.css  
http://192.168.1.4/dvwa/js/dvwaPage.js  
http://192.168.1.4/dvwa/css/source.css  
http://192.168.1.4/dvwa/includes/dvwaPage.inc.php  
http://192.168.1.4/dvwa/includes/DBMS/MySQL.php  
http://192.168.1.4/index.php  
http://192.168.1.4/dvwa/includes/DBMS/PGSQL.php  
http://192.168.1.4/dvwa/images/spanner.png  
http://192.168.1.4/setup.php  
http://192.168.1.4/external  
http://192.168.1.4/external/phpids/0.6  
http://192.168.1.4/external/recaptcha/recaptchalib.php  
http://192.168.1.4/security.php  
http://192.168.1.4/logout.php  
http://192.168.1.4/dvwa/images/login_logo.png  
http://192.168.1.4/dvwa/css/login.css  
http://192.168.1.4/login.php  
http://192.168.1.4/docs/pdf.html  
http://192.168.1.4/config/config.inc.php  
http://192.168.1.4/robots.txt  
http://192.168.1.4/Reports%20List  
http://192.168.1.4/Reports%20List.php  
http://192.168.1.4/docs/DVWA_v1.3.pdf  
http://192.168.1.4/dvwa/includes/dvwaPhpIds.inc.php  
http://192.168.1.4/dvwa/images/logo.png  
http://192.168.1.4/about.php  
http://192.168.1.4/favicon.ico  
http://192.168.1.4/instructions.php  
http://192.168.1.4/dvwa/images/RandomStorm.png  
http://192.168.1.4/dvwa/images/dollar.png  
http://192.168.1.4/dvwa/images/warning.png  
http://192.168.1.4/dvwa/css/help.css  
http://192.168.1.4/external%20files  
http://192.168.1.4/external%20files.php  
http://192.168.1.4/external%20files.txt  
http://192.168.1.4/dvwa/images/lock.png  
http://192.168.1.4/Style%20Library  
http://192.168.1.4/Style%20Library.txt  
http://192.168.1.4/modern%20mom  
http://192.168.1.4/modern%20mom.php  
http://192.168.1.4/neuf%20giga%20photo  
http://192.168.1.4/neuf%20giga%20photo.php  
http://192.168.1.4/neuf%20giga%20photo.txt  
http://192.168.1.4/phpinfo.php  
http://192.168.1.4/Web%20References.php  
http://192.168.1.4/Web%20References.txt  
http://192.168.1.4/COPYING.txt  
http://192.168.1.4/Contact%20Us
```

## Result output

If we want to log the output, we use the **--output** flag and then mentioning the file name.

```
feroxbuster -u http://192.168.1.4 --output results.txt
```

```
(root㉿kali)-[~]
# feroxbuster -u http://192.168.1.4 --output results.txt ←

|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
by Ben "epi" Risher 😊 ver: 2.10.4



|                   |                                           |
|-------------------|-------------------------------------------|
| 🎯 Target Url      | http://192.168.1.4                        |
| 🚀 Threads         | 50                                        |
| 📖 Wordlist        | /usr/share/seclists/Discovery/Web-Content |
| 🔥 Status Codes    | All Status Codes!                         |
| 🌟 Timeout (secs)  | 7                                         |
| 🦺 User-Agent      | feroxbuster/2.10.4                        |
| 📝 Config File     | /etc/feroxbuster/ferox-config.toml        |
| 🔍 Extract Links   | true                                      |
| 💾 Output File     | results.txt                               |
| 🚩 HTTP methods    | [GET]                                     |
| 🔃 Recursion Depth | 4                                         |


```

## User agent

To set up a custom user agent to send request at the server, we can use the **-a** or **--user-agent** flag. By default, the user agent used by Feroxbuster is **feroxbuster/<version>**.

```
feroxbuster -u http://192.168.1.4 -a "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
```

```
[root@Kali:~]# feroxbuster -u http://192.168.1.4 -a "Mozilla/5.0 (Windows NT 10.0; Win64; x64)" ←
[=][=][=)(=)[=][=]
by Ben "epi" Risher 😊
ver: 2.10.4

Target Url          http://192.168.1.4
Threads             50
Wordlist            /usr/share/seclists/Discovery/Web-Content/raft-medium-director
Status Codes        All Status Codes!
Timeout (secs)      7
User-Agent          Mozilla/5.0 (Windows NT 10.0; Win64; x64)
Config File         /etc/feroxbuster/ferox-config.toml
Extract Links       true
HTTP methods        [GET]
Recursion Depth    4
```

## Filter status code

There are times when we need to skip certain status codes responses, so we can use the **-C** or **--filter-status**, to skip the results of the mentioned codes. If we want to include a particular status code in output, we can use the **-s** or **--status-codes** flag.

```
feroxbuster -u http://192.168.1.4 -C 403,404
```

```
(root㉿kali)-[~]
# feroxbuster -u http://192.168.1.4 -C 403,404 ←

|__|__|__|_)|_)|_|_`   |__\|_\|_|_|_|\__|
|_|_|_|_|_\|_|_\|_|_`   |_\|/\|_|_|_|_|\__|
by Ben "epi" Risher 😊 ver: 2.10.4

◎ Target Url          http://192.168.1.4
🚀 Threads             50
📖 Wordlist            /usr/share/seclists/Discovery/Web-Content/raft-
☒ Status Code Filters [403, 404]
✳️ Timeout (secs)      7
crawler User-Agent     feroxbuster/2.10.4
📝 Config File          /etc/feroxbuster/ferox-config.toml
🔗 Extract Links       true
🏁 HTTP methods         [GET]
🔍 Recursion Depth    4

🏁 Press [ENTER] to use the Scan Management Menu™

404      GET      9l      32w      -c Auto-filtering found 404-like res
403      GET      11l     32w      -c Auto-filtering found 404-like res
301      GET      9l      28w      309c http://192.168.1.4/docs => http://
301      GET      9l      28w      311c http://192.168.1.4/config => http://
200      GET      47l     282w     1864c http://192.168.1.4/config/config.
200      GET      1l      10w      105c http://192.168.1.4/docs/pdf.html
200      GET      47l     282w     1859c http://192.168.1.4/config/config.
200      GET      0l      0w       0c http://192.168.1.4/config/config.
302      GET      0l      0w       0c http://192.168.1.4/ => login.php
301      GET      9l      28w      313c http://192.168.1.4/external => ht
301      GET      9l      28w      324c http://192.168.1.4/external/phpid
200      GET      0l      0w       0c http://192.168.1.4/external/recap
200      GET      2922l    17217w    730335c http://192.168.1.4/docs/DVWA_v1.3
[#####] - 6s      30014/30014  0s      found:11 errors:0
[#####] - 6s      30000/30000  5077/s  http://192.168.1.4/
[#####] - 0s      30000/30000  93458/s http://192.168.1.4/doc
[#####] - 0s      30000/30000  3000000/s http://192.168.1.4/c
[#####] - 0s      30000/30000  3750000/s http://192.168.1.4/e
[#####] - 0s      30000/30000  5000000/s http://192.168.1.4/e
[#####] - 1s      30000/30000  48309/s http://192.168.1.4/ext
```

## Quiet mode

To present the output without showing the progress bar or banner, we can use the quite mode by giving the **-q** or **--quiet** flag.

```
feroxbuster -u http://192.168.1.4 -q
```

```
(root㉿kali)-[~]
# feroxbuster -u http://192.168.1.4 -q ←

403      GET      11l      32w      -c Auto-filtering found 404-like
404      GET      9l       32w      -c Auto-filtering found 404-like
302      GET      0l       0w       0c http://192.168.1.4/ ⇒ login.php
301      GET      9l       28w      309c http://192.168.1.4/docs ⇒ http://192.168.1.4/docs/
301      GET      9l       28w      311c http://192.168.1.4/config ⇒ http://192.168.1.4/config/
200      GET      47l      282w     1864c http://192.168.1.4/config/config.inc.php.bak
200      GET      1l       10w      105c http://192.168.1.4/docs/pdf.pdf
301      GET      9l       28w      313c http://192.168.1.4/external/
301      GET      9l       28w      324c http://192.168.1.4/external/
200      GET      0l       0w       0c http://192.168.1.4/external/
404      GET      9l       33w      287c http://192.168.1.4/Reports%20
200      GET      2922l    17217w    730335c http://192.168.1.4/docs/DVWA
404      GET      9l       33w      289c http://192.168.1.4/external%
404      GET      9l       33w      288c http://192.168.1.4/Style%20L
200      GET      47l      282w     1859c http://192.168.1.4/config/config/
200      GET      0l       0w       0c http://192.168.1.4/config/config/
404      GET      9l       33w      285c http://192.168.1.4/modern%20
404      GET      9l       34w      290c http://192.168.1.4/neuf%20gi
404      GET      9l       33w      285c http://192.168.1.4/Contact%20
404      GET      9l       33w      286c http://192.168.1.4/Donate%20
```

## Controlling threads

To control the number of concurrent threads depending on the environment type, we can use the **--threads** or **-t** flag. The default threads value is 50.

```
feroxbuster -u http://192.168.1.4 -t 20
```

```
(root㉿kali)-[~]
# feroxbuster -u http://192.168.1.4 -t 20 ←

[██████████] [██████] [███████],  ██████████] / | | ██████████
by Ben "epi" Risher 🇪🇸 ver: 2.10.4

● Target Url          http://192.168.1.4
● Threads             20
● Wordlist            /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
● Status Codes        All Status Codes!
● Timeout (secs)      7
● User-Agent          feroxbuster/2.10.4
● Config File         /etc/feroxbuster/ferox-config.toml
● Extract Links       true
● HTTP methods        [GET]
● Recursion Depth    4

❖ Press [ENTER] to use the Scan Management Menu™

403      GET      11l      32w      -c Auto-filtering found 404-like response and created new f
404      GET      9l       32w      -c Auto-filtering found 404-like response and created new f
302      GET      0l       0w       0c http://192.168.1.4/ ⇒ login.php
301      GET      9l       28w      309c http://192.168.1.4/docs ⇒ http://192.168.1.4/docs/
301      GET      9l       28w      311c http://192.168.1.4/config ⇒ http://192.168.1.4/config/
200      GET      47l      282w     1859c http://192.168.1.4/config/config.inc.php.bak
```

## Custom wordlist

To use a custom wordlist, we can use the **-w** or **--wordlist** flag and then give the wordlist path. Here we are giving the **common.txt** file path.

```
feroxbuster -u http://192.168.1.4 -w /usr/share/wordlists/dirb/common.txt
```

```
(root㉿kali)-[~]
└─# feroxbuster -u http://192.168.1.4 -w /usr/share/wordlists/dirb/common.txt ↵

[!] FERXBUSTER [!]
by Ben "epi" Risher 🌐 ver: 2.10.4

● Target Url           http://192.168.1.4
● Threads              50
● Wordlist             /usr/share/wordlists/dirb/common.txt
● Status Codes          All Status Codes!
● Timeout (secs)        7
● User-Agent            feroxbuster/2.10.4
● Config File           /etc/feroxbuster/ferox-config.toml
● Extract Links         true
● HTTP methods          [GET]
● Recursion Depth       4

[!] Press [ENTER] to use the Scan Management Menu™

404      GET     91    32w      -c Auto-filtering found 404-like response and created new filte
403      GET     111   32w      -c Auto-filtering found 404-like response and created new filte
302      GET     01    0w       0c http://192.168.1.4/ ⇒ login.php
301      GET     91    28w      311c http://192.168.1.4/config ⇒ http://192.168.1.4/config/
200      GET     471   282w     1859c http://192.168.1.4/config/config.inc.php.bak
200      GET     471   282w     1864c http://192.168.1.4/config/config.inc.php.dist
200      GET     01    0w       0c http://192.168.1.4/config/config.inc.php
301      GET     91    28w      309c http://192.168.1.4/docs ⇒ http://192.168.1.4/docs/
404      GET     91    34w      297c http://192.168.1.4/Documents%20and%20Settings
200      GET     11    10w      105c http://192.168.1.4/docs/pdf.html
301      GET     91    28w      313c http://192.168.1.4/external ⇒ http://192.168.1.4/external/
200      GET     21    6w       1688c http://192.168.1.4/favicon.ico
```

## Disable recursion

To allow the scanning of only top level directories, we can set the **-n** or **--no-recursion** flag to disable the recursive scanning.

```
feroxbuster -u http://192.168.1.4 -n
```

```
(root㉿kali)-[~]
# feroxbuster -u http://192.168.1.4 -n ↪

[+] [+] [ ]) ( ) | /`| /` \`/ | | /` | /` 
by Ben "epi" Risher ☺
ver: 2.10.4

◎ Target Url          http://192.168.1.4
⚡ Threads              50
📅 Wordlist             /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
🔥 Status Codes         All Status Codes!
⌚ Timeout (secs)       7
🌐 User-Agent           feroxbuster/2.10.4
🔧 Config File          /etc/feroxbuster/ferox-config.toml
🌐 Extract Links        true
🌐 HTTP methods          [GET]
🚫 Do Not Recurse       true

※ Press [ENTER] to use the Scan Management Menu™

403   GET    11l    32w      -c Auto-filtering found 404-like response and created new filter
404   GET    9l     32w      -c Auto-filtering found 404-like response and created new filter
302   GET    0l     0w       0c http://192.168.1.4/ ⇒ login.php
301   GET    9l    28w      311c http://192.168.1.4/config ⇒ http://192.168.1.4/config/
301   GET    9l    28w      309c http://192.168.1.4/docs ⇒ http://192.168.1.4/docs/
301   GET    9l    28w      313c http://192.168.1.4/external ⇒ http://192.168.1.4/external/
404   GET    9l    33w      287c http://192.168.1.4/Reports%20List
404   GET    9l    33w      289c http://192.168.1.4/external%20files
404   GET    9l    33w      288c http://192.168.1.4/Style%20Library
404   GET    9l    33w      285c http://192.168.1.4/modern%20mom
404   GET    9l    34w      290c http://192.168.1.4/neuf%20giga%20photo
404   GET    9l    33w      289c http://192.168.1.4/Web%20References
404   GET    9l    33w      285c http://192.168.1.4/My%20Project
404   GET    0l    23w      285c http://192.168.1.4/contact%20us
```

## Limit recursion depth

To set a limit on the depth of recursion, we can use the `-L` or `--scan-limit`.

```
feroxbuster -u http://192.168.1.4 -L 4
```

```
(root㉿kali)-[~]
# feroxbuster -u http://192.168.1.4 -L 4 ←

|__|__|__|__|__| /`|__\ \_/_|_|_|_\ |__|
|__|__|__|__|__| \_/_| / \_|_|_|_|/_|_|__|
by Ben "epi" Risher 🇺🇸 ver: 2.10.4

◎ Target Url          http://192.168.1.4
🚀 Threads             50
📖 Wordlist            /usr/share/seclists/Discovery/Web-Co
🔥 Status Codes        All Status Codes!
✳️ Timeout (secs)     7
crawler User-Agent     feroxbuster/2.10.4
💉 Config File          /etc/feroxbuster/ferox-config.toml
🌐 Extract Links       true
🏁 HTTP methods         [GET]
🔃 Recursion Depth      4
🏆 Concurrent Scan Limit 4
```

## Force Recursion

To ensure that the recursion is used, we can use the **--force-recursion** flag.

```
feroxbuster -u http://192.168.1.4 --force-recursion
```

```
[root@kali)-[~]
# feroxbuster -u http://192.168.1.4 --force-recursion ←

[ERIK] by Ben "epi" Risher 😊 ver: 2.10.4

Target Url          http://192.168.1.4
Threads             50
Wordlist            /usr/share/seclists/Discovery/Web-Content/raft-medium-d
Status Codes        All Status Codes!
Timeout (secs)      7
User-Agent          feroxbuster/2.10.4
Config File         /etc/feroxbuster/ferox-config.toml
Extract Links       true
HTTP methods        [GET]
Recursion Depth    4
Force Recursion    true

Press [ENTER] to use the Scan Management Menu™

404      GET     9l     32w      -c Auto-filtering found 404-like response and
403      GET     11l    32w      -c Auto-filtering found 404-like response and
302      GET     0l     0w       0c http://192.168.1.4/ ⇒ login.php
301      GET     9l     28w     311c http://192.168.1.4/config ⇒ http://192.168.1.4/
301      GET     9l     28w     309c http://192.168.1.4/docs ⇒ http://192.168.1.4/
302      GET     2l     2w       0c http://192.168.1.4/config-ing.php
```

## Filter by character size

To filter out the messages of a particular length, we can use the **-S** or **--filter-size** flag. This will filter based on character size.

```
feroxbuster -u http://192.168.1.4 -q  
feroxbuster -u http://192.168.1.4 -q -S 285,286,283,289
```

```

└─(root㉿kali)-[~]
# feroxbuster -u http://192.168.1.4 -q ←

404      GET      9l      32w      -c Auto-filtering found 404-like response and
403      GET      11l     32w      -c Auto-filtering found 404-like response and
302      GET      0l      0w       0c http://192.168.1.4/ ⇒ login.php
301      GET      9l      28w      311c http://192.168.1.4/config ⇒ http://192.168.1.4/
200      GET      47l     282w     1859c http://192.168.1.4/config/config.inc.php.bak
200      GET      47l     282w     1864c http://192.168.1.4/config/config.inc.php.config
200      GET      0l      0w       0c http://192.168.1.4/config/config.inc.php.config
301      GET      9l      28w      313c http://192.168.1.4/external ⇒ http://192.168.1.4/
200      GET      0l      0w       0c http://192.168.1.4/external/recaptcha/recaptchacfg.php
301      GET      9l      28w      324c http://192.168.1.4/external/phpids/0.6 ⇒
404      GET      9l      33w      288c http://192.168.1.4/Style%20Library
301      GET      9l      28w      309c http://192.168.1.4/docs ⇒ http://192.168.1.4/
200      GET      1l      10w     105c http://192.168.1.4/docs/pdf.html
404      GET      9l      34w      290c http://192.168.1.4/neuf%20giga%20photo
404      GET      9l      33w      285c http://192.168.1.4/modern%20mom
200      GET      2922l    17217w   730335c http://192.168.1.4/docs/DVWA_v1.3.pdf
404      GET      9l      33w      285c http://192.168.1.4/Contact%20Us
404      GET      9l      33w      286c http://192.168.1.4/Donate%20Cash
404      GET      9l      33w      289c http://192.168.1.4/Planned%20Giving
404      GET      9l      33w      283c http://192.168.1.4/Site%20Map
404      GET      9l      33w      289c http://192.168.1.4/Privacy%20Policy
404      GET      9l      33w      287c http://192.168.1.4/Bequest%20Gift
404      GET      9l      33w      284c http://192.168.1.4/Gift%20Form
404      GET      9l      34w      291c http://192.168.1.4/Life%20Income%20Gift
404      GET      9l      33w      286c http://192.168.1.4/Site%20Assets
404      GET      9l      34w      286c http://192.168.1.4/What%20is%20New

Scanning: http://192.168.1.4/
⚠ Caught ctrl+c 🚫 saving scan state to ferox-http_192_168_1_4-1723366593.state ...
Scanning: http://192.168.1.4/
Scanning: http://192.168.1.4/config/
Scanning: http://192.168.1.4/external/
Scanning: http://192.168.1.4/external/phpids/
Scanning: http://192.168.1.4/external/recaptcha/
Scanning: http://192.168.1.4/docs/

└─(root㉿kali)-[~]
# feroxbuster -u http://192.168.1.4 -q -S 285,286,283,289 ←

403      GET      11l     32w      -c Auto-filtering found 404-like response and
404      GET      9l      32w      -c Auto-filtering found 404-like response and
302      GET      0l      0w       0c http://192.168.1.4/ ⇒ login.php
301      GET      9l      28w      309c http://192.168.1.4/docs ⇒ http://192.168.1.4/
301      GET      9l      28w      311c http://192.168.1.4/config ⇒ http://192.168.1.4/
200      GET      1l      10w     105c http://192.168.1.4/docs/pdf.html
200      GET      47l     282w     1864c http://192.168.1.4/config/config.inc.php.config
200      GET      47l     282w     1859c http://192.168.1.4/config/config.inc.php.config
200      GET      0l      0w       0c http://192.168.1.4/config/config.inc.php.config
301      GET      9l      28w      313c http://192.168.1.4/external ⇒ http://192.168.1.4/
301      GET      9l      28w      324c http://192.168.1.4/external/phpids/0.6 ⇒
200      GET      0l      0w       0c http://192.168.1.4/external/recaptcha/recaptchacfg.php
404      GET      9l      33w      287c http://192.168.1.4/Reports%20List
404      GET      9l      33w      288c http://192.168.1.4/Style%20Library
404      GET      9l      34w      290c http://192.168.1.4/neuf%20giga%20photo
200      GET      2922l    17217w   730335c http://192.168.1.4/docs/DVWA_v1.3.pdf
404      GET      9l      33w      284c http://192.168.1.4/Home%20Page
404      GET      9l      33w      287c http://192.168.1.4/Bequest%20Gift
404      GET      9l      33w      284c http://192.168.1.4/Gift%20Form
404      GET      9l      34w      291c http://192.168.1.4/Life%20Income%20Gift

Scanning: http://192.168.1.4/

```

## Filter by number of words

To filter out the results using number of words filter, we can use the **-w** or **--filter-words** flag.

```
feroxbuster -u http://192.168.1.4 -q  
feroxbuster -u http://192.168.1.4 -q -W 33
```

```

└─(root㉿kali)-[~]
# feroxbuster -u http://192.168.1.4 -q ←

```

403	GET	11l	32w	-c Auto-filtering found 40
404	GET	9l	32w	-c Auto-filtering found 40
302	GET	0l	0w	0c http://192.168.1.4/ ⇒
301	GET	9l	28w	309c http://192.168.1.4/docs
301	GET	9l	28w	311c http://192.168.1.4/config
200	GET	1l	10w	105c http://192.168.1.4/docs
200	GET	47l	282w	1864c http://192.168.1.4/config
301	GET	9l	28w	313c http://192.168.1.4/external/
301	GET	9l	28w	324c http://192.168.1.4/external/recaptcha/
200	GET	0l	0w	0c http://192.168.1.4/external/phpids/
404	GET	9l	33w	287c http://192.168.1.4/Repository
404	GET	9l	33w	289c http://192.168.1.4/external/
404	GET	9l	33w	288c http://192.168.1.4/Style
200	GET	47l	282w	1859c http://192.168.1.4/config
200	GET	0l	0w	0c http://192.168.1.4/config
404	GET	9l	34w	290c http://192.168.1.4/neuf
200	GET	2922l	17217w	730335c http://192.168.1.4/docs
404	GET	9l	33w	289c http://192.168.1.4/Web%
404	GET	9l	33w	285c http://192.168.1.4/My%
404	GET	9l	33w	286c http://192.168.1.4/Dona
404	GET	9l	33w	284c http://192.168.1.4/Home
404	GET	9l	33w	289c http://192.168.1.4/Plan
404	GET	9l	33w	289c http://192.168.1.4/Pres
404	GET	9l	33w	289c http://192.168.1.4/Priv
404	GET	9l	33w	283c http://192.168.1.4/Site
404	GET	9l	33w	284c http://192.168.1.4/Gift
404	GET	9l	33w	285c http://192.168.1.4/New%

Scanning: http://192.168.1.4/  
Caught **ctrl+c** 🚫 saving scan state to ferox-http\_192\_168\_1\_4-17

Scanning: http://192.168.1.4/  
Scanning: http://192.168.1.4/docs/  
Scanning: http://192.168.1.4/config/  
Scanning: http://192.168.1.4/external/  
Scanning: http://192.168.1.4/external/recaptcha/  
Scanning: http://192.168.1.4/external/phpids/

```

└─(root㉿kali)-[~]
# feroxbuster -u http://192.168.1.4 -q -W 33 ←

```

404	GET	9l	32w	-c Auto-filtering found 40
403	GET	11l	32w	-c Auto-filtering found 40
302	GET	0l	0w	0c http://192.168.1.4/ ⇒
301	GET	9l	28w	311c http://192.168.1.4/config
301	GET	9l	28w	309c http://192.168.1.4/docs
200	GET	47l	282w	1864c http://192.168.1.4/config
200	GET	47l	282w	1859c http://192.168.1.4/config
200	GET	0l	0w	0c http://192.168.1.4/config
301	GET	9l	28w	313c http://192.168.1.4/external/
200	GET	0l	0w	0c http://192.168.1.4/external/
301	GET	9l	28w	324c http://192.168.1.4/external/recaptcha/
200	GET	1l	10w	105c http://192.168.1.4/docs
404	GET	9l	34w	290c http://192.168.1.4/neuf
200	GET	2922l	17217w	730335c http://192.168.1.4/docs

Scanning: http://192.168.1.4/  
Caught **ctrl+c** 🚫 saving scan state to ferox-http\_192\_168\_1\_4-17

Scanning: http://192.168.1.4/  
Scanning: http://192.168.1.4/config/  
Scanning: http://192.168.1.4/docs/

## Filter by number of lines

To filter out the results using number of words filter, we can use the **-N** or **--filter-lines** flag.

```
feroxbuster -u http://192.168.1.4 -q  
feroxbuster -u http://192.168.1.4 -q -N 9
```

```

└──(root㉿kali)-[~]
# feroxbuster -u http://192.168.1.4 -q ←

```

Code	Method	Path	Size	Content
403	GET	11l	32w	-c Auto-filteri
404	GET	9l	32w	-c Auto-filteri
302	GET	0l	0w	0c http://192.1
301	GET	9l	28w	311c http://192.1
301	GET	9l	28w	309c http://192.1
200	GET	47l	282w	1859c http://192.1
200	GET	0l	0w	0c http://192.1
301	GET	9l	28w	313c http://192.1
200	GET	0l	0w	0c http://192.1
404	GET	9l	33w	287c http://192.1
200	GET	2922l	17217w	730335c http://192.1
200	GET	1l	10w	105c http://192.1
200	GET	47l	282w	1864c http://192.1
404	GET	9l	33w	288c http://192.1
301	GET	9l	28w	324c http://192.1
404	GET	9l	34w	290c http://192.1
404	GET	9l	33w	289c http://192.1
404	GET	9l	33w	285c http://192.1
404	GET	9l	33w	286c http://192.1
404	GET	9l	33w	284c http://192.1
404	GET	9l	33w	289c http://192.1
404	GET	9l	33w	289c http://192.1
404	GET	9l	33w	289c http://192.1
404	GET	9l	33w	283c http://192.1
404	GET	9l	33w	284c http://192.1
404	GET	9l	33w	286c http://192.1

Scanning: http://192.168.1.4/  
⚠ Caught **ctrl+c** ⚡ saving scan state to ferox-http\_192

Scanning: http://192.168.1.4/  
Scanning: http://192.168.1.4/config/  
Scanning: http://192.168.1.4/docs/  
Scanning: http://192.168.1.4/external/  
Scanning: http://192.168.1.4/external/recaptcha/  
Scanning: http://192.168.1.4/external/phpids/

```

└──(root㉿kali)-[~]
# feroxbuster -u http://192.168.1.4 -q -N 9 ←

```

Code	Method	Path	Size	Content
404	GET	9l	32w	-c Auto-filteri
403	GET	11l	32w	-c Auto-filteri
200	GET	1l	10w	105c http://192.1
302	GET	0l	0w	0c http://192.1
200	GET	2922l	17217w	730335c http://192.1
200	GET	47l	282w	1864c http://192.1
200	GET	47l	282w	1859c http://192.1
200	GET	0l	0w	0c http://192.1

Scanning: http://192.168.1.4/  
Scanning: http://192.168.1.4/docs/  
Scanning: http://192.168.1.4/config/  
Scanning: http://192.168.1.4/external/

## Filter by status code using deny list

To filter the results using status codes (deny list), we can use the **--filter-status** flag.

```
feroxbuster -u http://192.168.1.4 -q  
feroxbuster -u http://192.168.1.4 -q --filter-status 404
```

```

└─# feroxbuster -u http://192.168.1.4 -q ←
[404]   GET    9l      32w      -c Auto-filtering found 404
[403]   GET    11l     32w      -c Auto-filtering found 403
[301]   GET    9l      28w      309c http://192.168.1.4/docs
[200]   GET    1l      10w      105c http://192.168.1.4/docs
[301]   GET    9l      28w      313c http://192.168.1.4/exter
[200]   GET    0l      0w       0c http://192.168.1.4/exter
[301]   GET    9l      28w      324c http://192.168.1.4/exter
[302]   GET    0l      0w       0c http://192.168.1.4/ ⇒
[404]   GET    9l      33w      287c http://192.168.1.4/Repo
[404]   GET    9l      33w      288c http://192.168.1.4/Styl
[200]   GET    47l     282w     1859c http://192.168.1.4/cont
[200]   GET    0l      0w       0c http://192.168.1.4/cont
[301]   GET    9l      28w      311c http://192.168.1.4/cont
[200]   GET    47l     282w     1864c http://192.168.1.4/cont
[200]   GET    2922l   17217w   730335c http://192.168.1.4/docs
[404]   GET    9l      34w      290c http://192.168.1.4/neut
[404]   GET    9l      33w      289c http://192.168.1.4/Web%
[404]   GET    9l      33w      286c http://192.168.1.4/Dona
[404]   GET    9l      33w      284c http://192.168.1.4/Homes
[404]   GET    9l      33w      289c http://192.168.1.4/Priv
[404]   GET    9l      33w      289c http://192.168.1.4/Pres
[404]   GET    9l      33w      283c http://192.168.1.4/Site
[404]   GET    9l      33w      284c http://192.168.1.4/Gift
[404]   GET    9l      34w      291c http://192.168.1.4/Life
[404]   GET    9l      33w      285c http://192.168.1.4/New%
[404]   GET    9l      33w      286c http://192.168.1.4/Site

Scanning: http://192.168.1.4/
⚠ Caught ctrl+c ⚡ saving scan state to ferox-htt..._1_4-17
Scanning: http://192.168.1.4/
Scanning: http://192.168.1.4/docs/
Scanning: http://192.168.1.4/external/
Scanning: http://192.168.1.4/external/recaptcha/
Scanning: http://192.168.1.4/external/phpids/
Scanning: http://192.168.1.4/config/
Scanning: http://192.168.1.4/docs/pdf.html
Scanning: http://192.168.1.4/external/recaptcha/recaptchalib.php
Scanning: http://192.168.1.4/external/phpids/0.6
Scanning: http://192.168.1.4/config/config.inc.php.bak
Scanning: http://192.168.1.4/config/config.inc.php
Scanning: http://192.168.1.4/config/config.inc.php.dist
Scanning: http://192.168.1.4/docs/DVWA_v1.3.pdf

└──(root㉿kali)-[~]
└─# feroxbuster -u http://192.168.1.4 -q --filter-status 404 ←
[403]   GET    11l     32w      -c Auto-filtering found 403
[404]   GET    9l      32w      -c Auto-filtering found 404
[301]   GET    9l      28w      309c http://192.168.1.4/docs
[301]   GET    9l      28w      311c http://192.168.1.4/cont
[200]   GET    1l      10w      105c http://192.168.1.4/docs
[302]   GET    0l      0w       0c http://192.168.1.4/ ⇒
[200]   GET    47l     282w     1859c http://192.168.1.4/cont
[301]   GET    9l      28w      313c http://192.168.1.4/exter
[200]   GET    0l      0w       0c http://192.168.1.4/exter
[200]   GET    47l     282w     1864c http://192.168.1.4/cont
[301]   GET    9l      28w      324c http://192.168.1.4/exter
[200]   GET    2922l   17217w   730335c http://192.168.1.4/docs
[200]   GET    0l      0w       0c http://192.168.1.4/cont

Scanning: http://192.168.1.4/
Scanning: http://192.168.1.4/docs/
Scanning: http://192.168.1.4/config/

```

## Filter by status code using allow list

To filter the results using status codes (allow list), we can use the **--status-codes** flag.

```
feroxbuster -u http://192.168.1.4 -q  
feroxbuster -u http://192.168.1.4 -q --status-codes 200,301
```

```
└─(root㉿kali)-[~]
```

```
└─# feroxbuster -u http://192.168.1.4 -q ←
```

```
404      GET      9l      32w      -c Auto-filtering found 404-
403      GET      11l     32w      -c Auto-filtering found 404-
302      GET      0l      0w       0c http://192.168.1.4/ => lo
301      GET      9l      28w      311c http://192.168.1.4/config
200      GET      47l     282w     1864c http://192.168.1.4/config
200      GET      47l     282w     1859c http://192.168.1.4/config
200      GET      0l      0w       0c http://192.168.1.4/config
301      GET      9l      28w      313c http://192.168.1.4/extern
301      GET      9l      28w      324c http://192.168.1.4/extern
200      GET      0l      0w       0c http://192.168.1.4/extern
404      GET      9l      33w      287c http://192.168.1.4/Report
404      GET      9l      33w      289c http://192.168.1.4/extern
301      GET      9l      28w      309c http://192.168.1.4/docs =
200      GET      1l      10w      105c http://192.168.1.4/docs/p
404      GET      9l      33w      288c http://192.168.1.4/Style%
404      GET      9l      33w      285c http://192.168.1.4/modern
404      GET      9l      34w      290c http://192.168.1.4/neuf%2
200      GET      2922l    17217w   730335c http://192.168.1.4/docs/D
404      GET      9l      33w      285c http://192.168.1.4/My%20P
404      GET      9l      33w      285c http://192.168.1.4/Contac
404      GET      9l      33w      286c http://192.168.1.4/Donate
404      GET      9l      33w      289c http://192.168.1.4/Press%
404      GET      9l      33w      283c http://192.168.1.4/Site%2
404      GET      9l      33w      289c http://192.168.1.4/Planne
404      GET      9l      33w      284c http://192.168.1.4/Home%2
404      GET      9l      33w      283c http://192.168.1.4/About%
404      GET      9l      33w      287c http://192.168.1.4/Beques
Scanning: http://192.168.1.4/
⚠️ Caught ctrl+c ⚠️ saving scan state to ferox-http_192_168_1_4-1723
Scanning: http://192.168.1.4/
Scanning: http://192.168.1.4/config/
Scanning: http://192.168.1.4/external/
Scanning: http://192.168.1.4/external/recaptcha/
Scanning: http://192.168.1.4/external/phpids/
Scanning: http://192.168.1.4/docs/
```

```
└─(root㉿kali)-[~]
```

```
└─# feroxbuster -u http://192.168.1.4 -q --status-codes 200,301 ←
```

```
301      GET      9l      28w      309c http://192.168.1.4/docs =
301      GET      9l      28w      311c http://192.168.1.4/config
200      GET      0l      0w       0c http://192.168.1.4/config
200      GET      47l     282w     1864c http://192.168.1.4/config
200      GET      1l      10w      105c http://192.168.1.4/docs/p
200      GET      47l     282w     1859c http://192.168.1.4/config
200      GET      2922l    17217w   730335c http://192.168.1.4/docs/D
301      GET      9l      28w      313c http://192.168.1.4/extern
301      GET      9l      28w      324c http://192.168.1.4/extern
200      GET      0l      0w       0c http://192.168.1.4/extern
Scanning: http://192.168.1.4/
Scanning: http://192.168.1.4/config/
Scanning: http://192.168.1.4/docs/
Scanning: http://192.168.1.4/external/
Scanning: http://192.168.1.4/external/phpids/
Scanning: http://192.168.1.4/external/recaptcha/
```

## Generating random User-Agent

To use a random user agent for every request, we can use the **-A** flag. Here we have used the **--burp** flag simultaneously to show how the user agent looks in the requests.

```
feroxbuster -u http://192.168.1.4 -A --burp
```

```
[root@kali]~# feroxbuster -u http://192.168.1.4 -A --burp ←
[!] [!] [!] [!] [!]
by Ben "epi" Risher 😊
ver: 2.10.4

Target Url          http://192.168.1.4
Threads             50
Wordlist            /usr/share/seclists/Discovery/Web-Cont...
Status Codes        All Status Codes!
Timeout (secs)     7
User-Agent          Random
Config File         /etc/feroxbuster/ferox-config.toml
Proxy               http://127.0.0.1:8080
Extract Links       true
HTTP methods        [GET]
Insecure            true
Recursion Depth    4

Press [ENTER] to use the Scan Management Menu™

404      GET      9l      32w      -c Auto-filtering found 404
403      GET      11l     32w      -c Auto-filtering found 404
302      GET      0l      0w       0c http://192.168.1.4/ ⇒ l
301      GET      9l      28w     311c http://192.168.1.4/config

Burp Suite Community Edition v2024.5.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions
Intercept HTTP history WebSockets history | Proxy settings
Filter settings: Hiding CSS, image and general binary content

# ^ Host           Method URL                  Params Edited Status code Length MIME type Extension Title
1 https://api.github.com   GET   /repos/epi052/feroxbuster/releases... 200   26394 JSON
2 http://192.168.1.4     GET   /                      302   479   HTML
3 http://192.168.1.4     GET   /robots.txt          200   309   text   txt
4 http://192.168.1.4     GET   /                      302   478   HTML
5 http://192.168.1.4     GET   /e193d804561a4fab9eaf95ead23a... 404   587   HTML   404 Not Found
6 http://192.168.1.4     GET   /.htaccess13f862d2fb84794816b... 403   608   HTML   403 Forbidden
7 http://192.168.1.4     GET   /htaccessacebbd731121476fa1f4b5... 403   544   HTML   403 Forbidden
8 http://192.168.1.4     GET   /admin3b5834e5bed47c6b437c0... 404   529   HTML   404 Not Found
9 http://192.168.1.4     GET   /admin07fd621ed874491988f38... 404   592   HTML   404 Not Found
10 http://192.168.1.4    GET   /images              404   497   HTML   404 Not Found
11 http://192.168.1.4    GET   /sites               404   496   HTML   404 Not Found
12 http://192.168.1.4    GET   /img                 404   494   HTML   404 Not Found

Request
Pretty Raw Hex
1 GET /.htaccessacebbd731121476fa1f4b57451a08dcb HTTP/1.1
2 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.111 Safari/537.36
3 Accept: */*
4 Host: 192.168.1.4
5 Connection: keep-alive
6
7

Response
Pretty Raw Hex Render
1 HTTP/1.1 403 Forbidden
2 Date: Sun, 11 Aug 2024 09:18:52 GMT
3 Server: Apache/2.4.25 (Debian)
4 Content-Length: 327
5 Keep-Alive: timeout=5, max=100
6 Connection: Keep-Alive
7 Content-Type: text/html; charset=iso-8859-1
8
9 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"
10 <html>
11   <head>
12     <title>
```

## HTTP methods

To explicitly define the HTTP methods to be used, we can use the **-m** flag and then state the method to be used like POST. The default method is GET while running the Feroxbuster.

```
feroxbuster -u http://192.168.1.4 -m POST
```

```

└──(root㉿kali)-[~]
  # feroxbuster -u http://192.168.1.4 -m POST ↵

```

|\_\_|\_\_|\_\_|\_\_|\_\_|\_\_`|\_\_\|\_\_\|\_\_\|\_\_\|\_\_\|\_\_  
 |\_\_|\_\_|\_\_|\_\_\|\_\_\|\_\_\|\_\_\|\_\_\|\_\_\|\_\_\|\_\_  
 by Ben "epi" Risher 😊 ver: 2.10.4

---

🎯 Target Url	http://192.168.1.4
🚀 Threads	50
📖 Wordlist	/usr/share/seclists/Discovery/Web-Content/All Status Codes!
🔥 Status Codes	All Status Codes!
⌚ Timeout (secs)	7
.userAgent	feroxbuster/2.10.4
💉 Config File	/etc/feroxbuster/ferox-config.toml
🌐 Extract Links	true
🏁 HTTP methods	[POST]
🔃 Recursion Depth	4

---

🏁 Press [ENTER] to use the Scan Management Menu™

---

404	POST	9l	32w	-c Auto-filtering found 404
403	POST	11l	32w	-c Auto-filtering found 403
302	POST	0l	0w	0c http://192.168.1.4/ =>
301	POST	9l	28w	309c http://192.168.1.4/docs
200	GET	1l	10w	105c http://192.168.1.4/docs
301	POST	9l	28w	313c http://192.168.1.4/exte
200	GET	0l	0w	0c http://192.168.1.4/exte
301	GET	9l	28w	324c http://192.168.1.4/exte
404	GET	9l	32w	302c http://192.168.1.4/exte
404	GET	9l	32w	299c http://192.168.1.4/exte
404	POST	9l	33w	287c http://192.168.1.4/Repo
200	GET	2922l	17217w	730335c http://192.168.1.4/docs
404	POST	9l	33w	288c http://192.168.1.4/Styl
301	POST	9l	28w	311c http://192.168.1.4/conf
200	GET	0l	0w	0c http://192.168.1.4/conf
200	GET	47l	282w	1864c http://192.168.1.4/conf
404	POST	9l	33w	285c http://192.168.1.4/mode
404	POST	9l	34w	290c http://192.168.1.4/neuf
200	GET	47l	282w	1859c http://192.168.1.4/conf
404	POST	9l	33w	285c http://192.168.1.4/Cont
404	POST	9l	33w	286c http://192.168.1.4/Dona
404	POST	9l	33w	284c http://192.168.1.4/Home
404	POST	9l	33w	289c http://192.168.1.4/Plan
404	POST	9l	33w	289c http://192.168.1.4/Pres
404	POST	9l	33w	289c http://192.168.1.4/Priv
404	POST	9l	33w	283c http://192.168.1.4/Site
404	POST	9l	33w	284c http://192.168.1.4/Gift
404	POST	9l	34w	291c http://192.168.1.4/Life
404	POST	9l	33w	285c http://192.168.1.4/New%
404	POST	9l	33w	286c http://192.168.1.4/Site

[ #####>] - 4s    29991/30014    0s    found:28

## Custom headers

To explicitly define the request header to be used, we can use the **-H** flag and then state the header alongwith the value to be used like '**Content-Type: application/x-www-form-urlencoded**'. Here we have used the **--burp** flag simultaneously to show how the user agent looks in the requests.

```
feroxbuster -u http://192.168.1.4 -H 'Content-Type: application/x-www-form-urlencoded' --burp -q
```

The screenshot shows the Burp Suite interface. The top bar has the command: `# feroxbuster -u http://192.168.1.4 -H 'Content-Type: application/x-www-form-urlencoded' --burp -q`. The main window displays a list of network requests. A specific request to `/formulaires` is selected, highlighted with a red box. In the Request tab, the `Content-Type` header is also highlighted with a red box. The Response tab shows the server's response, which includes the `Content-Type: text/html; charset=iso-8859-1` header. The Inspector tab shows the request attributes, headers, and response headers. The Notes tab is visible on the right.

## Cookies

To use a specific cookie value in all the requests, we can mention the cookies header alongwith the value. The flag which can be used here is **--cookies** or **-b**. Here we have used the **--burp** flag simultaneously to show how the cookie looks in the requests.

```
feroxbuster -u http://192.168.1.4 --cookies PHPSESSID=t54ij15l5d51i2tc7j1k1tu4p4 --burp -q
```

```
[root@kali:~]# feroxbuster -u http://192.168.1.4 --cookies PHPSESSID=t54ijj15l5d51i2tc7j1k1tu4p4 --burp -q ↵
404      GET      91       32w      -c Auto-filtering found 404-like response and created new filter; to
403      GET      111      32w      -c Auto-filtering found 404-like response and created new filter; to
302      GET      01       0w       0c http://192.168.1.4/ ⇒ login.php
301      GET      91       28w      309c http://192.168.1.4/docs ⇒ http://192.168.1.4/docs/
301      GET      91       28w      311c http://192.168.1.4/config => http://192.168.1.4/config/
200      GET      1l       10w      105c http://192.168.1.4/docs/pdf.html
200      GET      01       0w       0c http://192.168.1.4/config/config.inc.php
200      GET      171      282w     1850c http://192.168.1.4/config/config.inc.php.html
5

Bur Suite Community Edition v2024.5.5 - Temporary Project
Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Filter settings: Hiding CSS, image and general binary content
# ▾ Host Met... URL Param... Edited Status c... Len... MIME ... Extens... Title Notes TLS IP Cookies Time Listener
2... http://192.168.1.4 GET /ron 404 494 HTML 404 Not Found 192.168.1.4 05:42:1... 8080
2... http://192.168.1.4 GET /sdx 404 494 HTML 404 Not Found 192.168.1.4 05:42:1... 8080
2... http://192.168.1.4 GET /searchedit 404 501 HTML 404 Not Found 192.168.1.4 05:42:1... 8080
2... http://192.168.1.4 GET /rechercher 404 501 HTML 404 Not Found 192.168.1.4 05:42:1... 8080
2... http://192.168.1.4 GET /scripts2 404 499 HTML 404 Not Found 192.168.1.4 05:42:1... 8080
2... http://192.168.1.4 GET /reserv 404 497 HTML 404 Not Found 192.168.1.4 05:42:1... 8080
2... http://192.168.1.4 GET /riders 404 497 HTML 404 Not Found 192.168.1.4 05:42:1... 8080
2... http://192.168.1.4 GET /seasonal 404 499 HTML 404 Not Found 192.168.1.4 05:42:1... 8080
2... http://192.168.1.4 GET /searchprofile 404 504 HTML 404 Not Found 192.168.1.4 05:42:1... 8080
2... http://192.168.1.4 GET /rsscache 404 499 HTML 404 Not Found 192.168.1.4 05:42:1... 8080
2... http://192.168.1.4 GET /schulung 404 499 HTML 404 Not Found 192.168.1.4 05:42:1... 8080

Request Response Inspector
Pretty Raw Hex Pretty Raw Hex Render Request attributes 2
1 GET /rsscache HTTP/1.1 1 HTTP/1.1 404 Not Found Request cookies 1
2 Accept: */* 2 Date: Sun, 11 Aug 2024 09:42:11 GMT Request headers 5
3 User-Agent: feroxbuster/2.10.4 3 Server: Apache/2.4.25 (Debian)
4 Cookie: PHPSESSID=t54ijj15l5d51i2tc7j1k1tu4p4 4 Content-Length: 283 Response headers 6
5 Host: 192.168.1.4 5 Keep-Alive: timeout=5, max=62
6 Connection: Keep-Alive
```

## Adding slash

To add a slash (/) after every request, we can use the **-f** or **--add-slash** flag.

```
feroxbuster -u http://192.168.1.4 -f
```

## Capturing requests in Burp

To capture a request in Burp Suite, we can use the **--burp** flag while running the scan.

```
feroxbuster -u http://192.168.1.4 –burp
```

## Read target from list

To perform the scanning on the targets provided in the list, we can use the following command:

```
cat target.txt  
cat target.txt | feroxbuster --stdin -q
```

```
(root㉿kali)-[~]  
# cat target.txt  
http://192.168.1.4  
https://google.com  
http://192.168.1.5
```

```
(root㉿kali)-[~]  
# cat target.txt | feroxbuster --stdin -q ←
```

Could not connect to http://192.168.1.5, skipping ...  
⇒ error sending request for url (http://192.168.1.5/)

Code	Method	Length	Time	Content
404	GET	9l	32w	-c Auto-filtering found 404-like re
403	GET	11l	32w	-c Auto-filtering found 404-like re
302	GET	0l	0w	0c http://192.168.1.4/ ⇒ login.php
301	GET	9l	28w	309c http://192.168.1.4/docs ⇒ http:
301	GET	9l	28w	311c http://192.168.1.4/config ⇒ htt
200	GET	1l	10w	105c http://192.168.1.4/docs/pdf.html
200	GET	47l	282w	1864c http://192.168.1.4/config/config
200	GET	0l	0w	0c http://192.168.1.4/config/config
301	GET	9l	28w	313c http://192.168.1.4/external ⇒ h
200	GET	0l	0w	0c http://192.168.1.4/external/reca
301	GET	9l	28w	324c http://192.168.1.4/external/phpi
301	GET	6l	14w	225c https://google.com/labs/ ⇒ http
301	GET	6l	14w	231c https://google.com/nonprofits/ =
301	GET	6l	14w	235c https://google.com/commercesearc
301	GET	6l	14w	226c https://google.com/forms/ ⇒ htt
301	GET	6l	14w	268c https://google.com/about/careers
301	GET	6l	14w	257c https://google.com/about/careers
301	GET	6l	14w	227c https://google.com/scholar ⇒ ht
301	GET	6l	14w	258c https://google.com/about/careers
301	GET	6l	14w	233c https://google.com/trends/topics
301	GET	6l	14w	260c https://google.com/about/careers
301	GET	6l	14w	235c https://google.com/hotelfinder/r
301	GET	6l	14w	240c https://google.com/landing/cmsne
301	GET	6l	14w	249c https://google.com/help/maps/ind
301	GET	6l	14w	228c https://google.com/books/ ⇒ htt
301	GET	6l	14w	257c https://google.com/adsense/ ⇒ ht

## Resume from last state

If we wish to resume the scan from the last state, we can use the **--resume-from** flag and provide the **.state** file. There are times when we need to terminate the scan in between, so Feroxbuster will save the results in the file.

```
feroxbuster -u http://192.168.1.4 -q  
feroxbuster --resume-from ferox-http_192_168_1_4-1723370176.state -q
```

```
(root㉿kali)-[~]
# feroxbuster -u http://192.168.1.4 -q ←

404      GET      9l      32w      -c Auto-filtering found 404-like response
403      GET      11l     32w      -c Auto-filtering found 404-like response
302      GET      0l      0w       0c http://192.168.1.4/ => login.php
301      GET      9l      28w      309c http://192.168.1.4/docs => http://192.1
301      GET      9l      28w      311c http://192.168.1.4/config => http://192.1
200      GET      1l      10w     105c http://192.168.1.4/docs/pdf.html
200      GET      47l     282w    1864c http://192.168.1.4/config/config.inc.ph
200      GET      47l     282w    1859c http://192.168.1.4/config/config.inc.ph
200      GET      0l      0w       0c http://192.168.1.4/config/config.inc.ph
301      GET      9l      28w      313c http://192.168.1.4/external => http://1
301      GET      9l      28w      324c http://192.168.1.4/external/phpids/0.6
200      GET      0l      0w       0c http://192.168.1.4/external/recaptcha/r
404      GET      9l      33w      287c http://192.168.1.4/Reports%20List
404      GET      9l      33w      289c http://192.168.1.4/external%20files
404      GET      9l      33w      288c http://192.168.1.4/Style%20Library
404      GET      9l      33w      285c http://192.168.1.4/modern%20mom
404      GET      9l      34w      290c http://192.168.1.4/neuf%20giga%20photo
Scanning: http://192.168.1.4/
⚠ Caught ctrl+c ⚠ saving scan state to ferox-http_192_168_1_4-1723370176.state .

Scanning: http://192.168.1.4/
Scanning: http://192.168.1.4/config/
Scanning: http://192.168.1.4/external/
Scanning: http://192.168.1.4/external/recaptcha/
Scanning: http://192.168.1.4/external/phpids/

(root㉿kali)-[~]
# feroxbuster --resume-from ferox-http_192_168_1_4-1723370176.state -q ←

302      GET      0l      0w       0c http://192.168.1.4/ => login.php
301      GET      9l      28w      309c http://192.168.1.4/docs => http://192.1
301      GET      9l      28w      311c http://192.168.1.4/config => http://192.1
200      GET      1l      10w     105c http://192.168.1.4/docs/pdf.html
200      GET      47l     282w    1864c http://192.168.1.4/config/config.inc.ph
200      GET      47l     282w    1859c http://192.168.1.4/config/config.inc.ph
200      GET      0l      0w       0c http://192.168.1.4/config/config.inc.ph
301      GET      9l      28w      313c http://192.168.1.4/external => http://1
301      GET      9l      28w      324c http://192.168.1.4/external/phpids/0.6
200      GET      0l      0w       0c http://192.168.1.4/external/recaptcha/r
404      GET      9l      33w      287c http://192.168.1.4/Reports%20List
404      GET      9l      33w      289c http://192.168.1.4/external%20files
404      GET      9l      33w      288c http://192.168.1.4/Style%20Library
404      GET      9l      33w      285c http://192.168.1.4/modern%20mom
404      GET      9l      34w      290c http://192.168.1.4/neuf%20giga%20photo
404      GET      9l      32w      -c Auto-filtering found 404-like response
403      GET      11l     32w      -c Auto-filtering found 404-like response
200      GET      2922l    17217w   730335c http://192.168.1.4/docs/DVWA_v1.3.pdf
404      GET      9l      33w      285c http://192.168.1.4/Contact%20Us
404      GET      9l      33w      286c http://192.168.1.4/Donate%20Cash
404      GET      9l      33w      284c http://192.168.1.4/Home%20Page
404      GET      9l      33w      289c http://192.168.1.4/Planned%20Giving
404      GET      9l      33w      283c http://192.168.1.4/Site%20Map
Scanning: http://192.168.1.4/config/
⚠ Caught ctrl+c ⚠ saving scan state to ferox-http_192_168_1_4-1723370197.state .
Scanning: http://192.168.1.4/config/
Scanning: http://192.168.1.4/external/
Scanning: http://192.168.1.4/external/recaptcha/
Scanning: http://192.168.1.4/external/phpids/
Scanning: http://192.168.1.4/docs/
```

## Follow redirect

While scanning if there are requests which result in the redirection, so we can control that by allowing the clients to follow the redirects using -r flag.

```
feroxbuster -u http://192.168.1.4 -r
```

```
(root㉿kali)-[~]
# feroxbuster -u http://192.168.1.4 -r ↵

[+] [+] [+] [+] [+] [+] [+] [+] [+] [+] [+] [+] [+] [+]
by Ben "epi" Risher 😊 ver: 2.10.4

[?] Target Url           http://192.168.1.4
[?] Threads              50
[?] Wordlist             /usr/share/seclists/Discovery/Web-Content/raft-medium-direc
[?] Status Codes          All Status Codes!
[?] Timeout (secs)        7
[?] User-Agent            feroxbuster/2.10.4
[?] Config File           /etc/feroxbuster/ferox-config.toml
[?] Extract Links         true
[?] HTTP methods          [GET]
[?] Follow Redirects      true
[?] Recursion Depth       4

[?] Press [ENTER] to use the Scan Management Menu™

403   GET    11l    32w      -c Auto-filtering found 404-like response and cr
404   GET    9l     32w      -c Auto-filtering found 404-like response and cr
200   GET    59l    101w     842c http://192.168.1.4/dvwa/css/login.css
200   GET    1l     10w      105c http://192.168.1.4/docs/pdf.html
200   GET    18l    95w      8064c http://192.168.1.4/dvwa/images/RandomStorm.pn
200   GET    0l     0w       0c http://192.168.1.4/config/config.inc.php
200   GET    47l    282w     1859c http://192.168.1.4/config/config.inc.php.bak
200   GET    47l    282w     1864c http://192.168.1.4/config/config.inc.php.dist
200   GET    0l     0w       0c http://192.168.1.4/external/recaptcha/recaptc
200   GET    165l   1234w    7639c http://192.168.1.4/external/phpids/0.6/LICENSE
200   GET    18l    24w      380c http://192.168.1.4/external/phpids/0.6/build.
404   GET    9l     33w      287c http://192.168.1.4/Reports%20List
404   GET    9l     33w      289c http://192.168.1.4/external%20files
404   GET    9l     33w      288c http://192.168.1.4/Style%20Library
200   GET    25l    36w      304c http://192.168.1.4/dvwa/css/help.css
200   GET    20l    29w      240c http://192.168.1.4/dvwa/css/source.css
200   GET    266l   486w     4026c http://192.168.1.4/dvwa/css/main.css
200   GET    39l    244w    16182c http://192.168.1.4/dvwa/images/login_logo.png
200   GET    77l    129w    1523c http://192.168.1.4/login.php
200   GET    24l    62w      593c http://192.168.1.4/dvwa/js/add_event_listener
200   GET    39l    99w      1030c http://192.168.1.4/dvwa/js/dvwaPage.js
404   GET    9l     33w      285c http://192.168.1.4/modern%20mom
404   GET    9l     34w      290c http://192.168.1.4/neuf%20giga%20photo
```

## Timeout

To setup a timeout limit, we can use the `-T` flag. This determines the amount of time the Feroxbuster will wait for the server response before terminating the request.

scan. By default, this value is set to 7 seconds, however we can modify it by using the flag.

```
feroxbuster -u http://192.168.1.4
```

```
(root㉿kali)-[~]
# feroxbuster -u http://192.168.1.4 ←

[+] [+] [+] ) [+] ) [+] /` [+] \ [+] / [+] \
by Ben "epi" Risher 😊 [+] \ [+] / [+] / [+] \
ver: 2.10.4

Target Url: http://192.168.1.4
Threads: 50
Wordlist: /usr/share/seclists/Discovery
Status Codes: All Status Codes!
Timeout (secs): 7
User-Agent: feroxbuster/2.10.4
Config File: /etc/feroxbuster/ferox-config
Extract Links: true
HTTP methods: [GET]
Recursion Depth: 4
```

The above image shows the default timeout limit used and now we are going to modify it to 5 seconds.

```
feroxbuster -u http://192.168.1.4 -T 5
```

```

└─(root㉿kali)-[~]
# feroxbuster -u http://192.168.1.4 -T 5 ←

```

---	---	---	---	---	---	---	---

by Ben "epi" Risher 😊 ver: 2.10.4

🎯 Target Url	http://192.168.1.4
🚀 Threads	50
📖 Wordlist	/usr/share/seclists/Discovery/All Status Codes!
🔥 Status Codes	<b>5</b>
⚡ Timeout (secs)	feroxbuster/2.10.4
_MOUSE User-Agent	/etc/feroxbuster/ferox-con
💉 Config File	true
🔍 Extract Links	[GET]
🏁 HTTP methods	4
🔃 Recursion Depth	

## Comparasion between Feroxbuster and other tools

- **Feroxbuster** stands out for its comprehensive set of features, including extensive response filtering, Burp Suite integration, and customization options. It provides a balance between advanced functionality and user control, making it a powerful choice for detailed and nuanced directory and file brute-forcing.
- **DirBuster** is user-friendly with its GUI but may not be as fast or flexible as command-line tools like Feroxbuster.
- **Gobuster** offer speed and efficiency but with fewer advanced features and less flexibility compared to Feroxbuster.
- **ffuf** provides high performance and extensive filtering but can be complex to configure and use.

## Conclusion

In conclusion, we can say that **Feroxbuster** is an excellent choice for those requiring precise control over their scanning processes, advanced filtering capabilities, and the ability to integrate with other tools.

# JOIN OUR TRAINING PROGRAMS

**CLICK HERE**

## BEGINNER

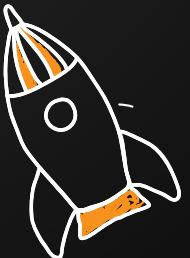
Ethical Hacking

Bug Bounty

Network Security Essentials

Network Pentest

Wireless Pentest



## ADVANCED

Burp Suite Pro

Web Services-API

Pro Infrastructure VAPT

Computer Forensics

Android Pentest

Advanced Metasploit

CTF



## EXPERT

Red Team Operation

Privilege Escalation

- APT's - MITRE Attack Tactics
- Active Directory Attack
- MSSQL Security Assessment

- Windows
- Linux

