# **GOITE** Technologies

# A Detailed Guide on Feroxbuster

www.ignitetechnologies.in



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



#### 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
```

(	—_( <b>root®kali</b> )-[~] —# feroxbuster -u http://192.168.1.4								
 ) ру В	)      \  en "epi" Ris	)   /   \   \_ sher ☺	_, //	\_/     \   / \    /   ver: 2.10.4					
© ∦ ♦ ♦ ₩ ₩ ₩	Target Url Threads Wordlist Status Code Timeout (se User-Agent Config File Extract Lin HTTP methoo Recursion D	es ecs) e ks ls eepth	http:/ 50 /usr/s All St 7 feroxb /etc/f true [GET] 4	/192.168.1.4 hare/seclists/Discovery/Web-Content/raft-medium-directories.txt atus Codes! uster/2.10.4 eroxbuster/ferox-config.toml					
pss	Press [ENTE	R] to use	e the <mark>Scan</mark>	Management Menu™					
+03 +04 302 301 200 301 200 301 200	GET GET GET GET GET GET GET GET	111 91 01 91 471 91 91 01	32w 32w 0w 28w 28w 282w 282w 28w 28w 28w 0w	<pre>-c Auto-filtering found 404-like response and created new filt -c Auto-filtering found 404-like response and created new filt 0c http://192.168.1.4/ ⇒ login.php 309c http://192.168.1.4/docs ⇒ http://192.168.1.4/docs/ 311c http://192.168.1.4/config =&gt; http://192.168.1.4/config/ 1859c http://192.168.1.4/config/config.inc.php.bak 313c http://192.168.1.4/external ⇒ http://192.168.1.4/external/ 324c http://192.168.1.4/external/phpids/0.6 ⇒ http://192.168.1.4/external/ 0c http://192.168.1.4/external/recaptchalib.php</pre>					
04	GET	91	33w	289c http://192.168.1.4/external%20files					

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://192.168.1.4silent
---

(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

<b>(</b>	[(root@kali)-[~] _# feroxbuster -u http://192.168.1.4 -r ◀━━								
l l by B	)     \ en "epi" R	) /   \ \_ isher @	_, /_\ _, \_/	<pre>\_/     \_   /    /   ver: 2.10.4</pre>					
© % • • * * * *	Target Ur Threads Wordlist Status Co Timeout ( User-Agen Config Fi Extract L HTTP meth Follow Re Recursion	l des secs) t le inks ods directs Depth	http: 50 /usr/ All S 7 ferox /etc/ true [GET] true 4	//192.168.1.4 share/seclists/Discovery/Web-Content/raft-medium-directories tatus Codes! ouster/2.10.4 feroxbuster/ferox-config.toml	.txt				
<i>₿</i> ≋≋	Press [EN	TER] to us	e the Scan	Management Menu <sup>m</sup>					
404 403 200 200	GET GET GET	9l 11l 47l 471	32w 32w 282w 282w	<pre>-c Auto-filtering found 404-like response and created -c Auto-filtering found 404-like response and created 1864c http://192.168.1.4/config/config.inc.php.dist 1859c http://192.168.1.4/config/config.inc.php.bak</pre>	new new				
200	GET	471 0l	202w Øw	0c http://192.168.1.4/config/config.inc.php.bak					
200	GET	11	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	391	244w	16182c http://192.168.1.4/dvwa/images/login_logo.png					
200	GET	01	Øw	<pre>0c http://192.168.1.4/external/recaptcha/recaptchalib.</pre>	php				
200	GET	165l	1234w	7639c http://192.168.1.4/external/phpids/0.6/LICENSE					
200	GET	29221	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

-# 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.



#### 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)"



#### 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

	<mark>──(root⊛kali</mark> )-[~] └─# feroxbuster -u http://192.168.1.4 -C 403,404 - <b>4</b>								
   by B	)      \  en "epi" Ris	)   /_`` \   sher 🤓		\_/     / \    / ver: 2	 /   2.10.4				
© 🔌 🖩 💢 ±	Target Url Threads Wordlist Status Code Timeout (se User-Agent Config File Extract Lin HTTP methoo Recursion [	e Filters ecs) hks ds Depth	http: 50 /usr/ [403, 7 ferox /etc/ true [GET] 4	<pre>http://192.168.1.4 50 /usr/share/seclists/Discovery/Web-Content/raft- [403, 404] 7 feroxbuster/2.10.4 /etc/feroxbuster/ferox-config.toml true [GET] 4</pre>					
<b>p</b> 888	Press [ENTE	R] to use	the Scan	Management	t Menu™				
404 403 301 200 200 200 200 302 301 301	GET GET GET GET GET GET GET GET GET	91 111 91 471 11 471 01 91 91	32w 32w 28w 28w 282w 10w 282w 0w 282w 0w 28w 28w	-c Au -c Au 309c ht 311c ht 1864c ht 105c ht 1859c ht 0c ht 313c ht 324c ht	Ito-filte Ito-filte Itp://192 Itp://192 Itp://192 Itp://192 Itp://192 Itp://192 Itp://192 Itp://192	ering found 40 ering found 40 2.168.1.4/docs 2.168.1.4/con 2.168.1.4/con 2.168.1.4/con 2.168.1.4/con 2.168.1.4/con 2.168.1.4/con 2.168.1.4/exto 2.168.1.4/exto	04-like res 04-like res s ⇒ http:/ fig => http fig/config. s/pdf.html fig/config. fig/config. login.php ernal ⇒ ht		
200 200 [#### [#### [#### [#### [####	GET GET	0l 2922l 5 ######] - 69 ######] - 69 #######] - 09 #######] - 09 #######] - 09 ########] - 1	0w 5 30 5 30 5 30 5 30 5 30 5 30 5 30 5 30	0c ht 730335c ht 014/30014 000/30000 000/30000 000/30000 000/30000 000/30000	tp://192 0s 5077/s 93458/s 3000000 3750000 5000000 48309/s	2.168.1.4/ext 2.168.1.4/doc found:11 http://192.2 s http://192.2 0/s http://192 0/s http://192 0/s http://192.2	ernal/recap s/DVWA_v1.3 errors:0 168.1.4/ 168.1.4/doc 2.168.1.4/c 2.168.1.4/e 2.168.1.4/e 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

(rootskali)-[~]								
L_#	feroxbuster	-u http:	//192.168.	1.4 -q 🚽				
403	GET	11l	32w	– c	Auto-filtering found 404-lik			
404	GET	91	32w	- C	Auto-filtering found 404-lik			
302	GET	0l	Øw	0c	http://192.168.1.4/ ⇒ login			
301	GET	91	28w	311c	http://192.168.1.4/config $\Rightarrow$			
301	GET	91	28w	309c	http://192.168.1.4/docs $\Rightarrow$ h			
200	GET	47l	282w	1864c	http://192.168.1.4/config/co			
200	GET	11	10w	105c	http://192.168.1.4/docs/pdf.			
301	GET	91	28w	313c	http://192.168.1.4/external			
301	GET	91	28w	324c	http://192.168.1.4/external/			
200	GET	01	0w	0c	http://192.168.1.4/external/			
404	GET	91	33w	287c	http://192.168.1.4/Reports%2			
200	GET	2922l	17217w	730335c	http://192.168.1.4/docs/DVWA			
404	GET	91	33w	289c	http://192.168.1.4/external%			
404	GET	91	33w	288c	http://192.168.1.4/Style%20L			
200	GET	47l	282w	1859c	http://192.168.1.4/config/co			
200	GET	01	0w	0c	http://192.168.1.4/config/co			
404	GET	91	33w	285c	http://192.168.1.4/modern%20			
404	GET	91	34w	290c	http://192.168.1.4/neuf%20gi			
404	GET	91	33w	285c	http://192.168.1.4/Contact%2			
404	GET	91	33w	2860	httn://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
```

<b>(</b>	——( <b>root⊛kali</b> )-[~] —# feroxbuster -u http://192.168.1.4 -t 20 <del>→</del>								
I I by B	)       \   en "epi" Risk	_)   / `` \   ner @	/\ \/	\_/     \   / \    /   ver: 2.10.4					
© % • • • • •	<ul> <li>Target Url</li> <li>Threads</li> <li>Wordlist</li> <li>Status Codes</li> <li>Timeout (secs)</li> <li>User-Agent</li> <li>Config File</li> <li>Extract Links</li> </ul>			//192.168.1.4 hare/seclists/Discovery/Web-Content/raft-medium-directories.txt atus Codes! puster/2.10.4 feroxbuster/ferox-config.toml					
<u>N</u>	Recursion De	epth 	4						
<b>P</b> 88	Press [ENTER	R] to use	the Scan	Management Menu™					
403 404	GET GET	11l 9l	32w 32w	<ul> <li>-c Auto-filtering found 404-like response and created new f</li> <li>-c Auto-filtering found 404-like response and created new f</li> </ul>					
302 301 301	GET GET GET	01 91 91	0w 28w 28w	0c http://192.168.1.4/ → login.php 309c http://192.168.1.4/docs → http://192.168.1.4/docs/ 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					

# **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



#### **Disable recursion**

To allow the scanning of only top level directories, we can set the **-n** or **--norecursion** flag to disable the recursive scanning.

feroxbuster -u http://192.168.1.4 -n	

	(root@ kali)-[~]								
   by B		)   /` )   /` \		<pre>/ - / - / - / - / - / - / - / - / - / -</pre>					
© ∦ ■ • • • • • • • • • • •	Target Url Threads Wordlist Status Code Timeout (se User-Agent Config File Extract Lin HTTP method Do Not Recu	es ecs) eks ls erse	http:// 50 /usr/s All St. 7 feroxb /etc/f true [GET] true	/192.168.1.4 hare/seclists/Discovery/Web-Content/raft-medium-directories.txt atus Codes! uster/2.10.4 eroxbuster/ferox-config.toml					
	Press [ENTE	R] to use	the Scan I	Management Menu™					
403 404 302 301 301 301 404 404	GET GET GET GET GET GET GET GET	111 91 01 91 91 91 91 91	32w 32w 0w 28w 28w 28w 33w 33w	<pre>-c Auto-filtering found 404-like response and created new filter -c Auto-filtering found 404-like response and created new filter 0c http://192.168.1.4/ ⇒ login.php 311c http://192.168.1.4/config ⇒ http://192.168.1.4/config/ 309c http://192.168.1.4/docs ⇒ http://192.168.1.4/docs/ 313c http://192.168.1.4/external ⇒ http://192.168.1.4/external/ 287c http://192.168.1.4/external%20List 289c http://192.168.1.4/external%20Files</pre>					
404 404 404 404 404	GET GET GET GET GET	91 91 91 91 91 91	33w 33w 34w 33w 33w	288c http://192.168.1.4/Style%20Library 285c http://192.168.1.4/modern%20mom 290c http://192.168.1.4/neuf%20giga%20photo 289c http://192.168.1.4/Web%20References 285c http://192.168.1.4/My%20Project					

# 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
```



#### **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



#### 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
```

	<mark>oot⊛kali</mark> ) eroxbuster	-[~] u http:/	//192.168.	.1.4 -a 🛶
	C F T	01	22.	·
	GEI	9L	32w	-c Auto-filtering found 404-like response and
403	GET	11L 01	32W 0w	$-c$ Auto-fittering found 404-like response and $ac$ http://102.168.1.4/ $\rightarrow$ login php
302	GET	91	28W	$311c \text{ http://192.108.1.4/ } \rightarrow \text{ togin.php}$
200	GET	471	282w	1859c http://192.168.1.4/config/config.inc.php.l
200	GET	471	282w	1864c http://192.168.1.4/config/config.inc.php.0
200	GET	01	Øw	0c http://192.168.1.4/config/config.inc.php
301	GET	91	28w	313c http://192.168.1.4/external $\Rightarrow$ http://192
200	GET	01	Øw	<pre>0c http://192.168.1.4/external/recaptcha/reca</pre>
301	GET	91	28w	324c http://192.168.1.4/external/phpids/0.6 $\Rightarrow$
	GET	91	33w	288c http://192.168.1.4/Style%20Library
301	GET	91	28w	$309c \text{ http://192.168.1.4/docs} \Rightarrow \text{ http://192.168}$
200	GEI	11	10w	105c http://192.168.1.4/docs/pdf.html
	GET	91	34W	290C http://192.168.1.4/neuf%20g1ga%20pnoto
404	GET	9L 20221	یر 17017w	205C Http://192.100.1.4/modern&20mm 730335c http://192 168 1 4/docs/DVWA v1 3 pdf
404	GET	91	33w	285c http://192.168.1.4/Contact%20Us
	GET	91	33w	286c http://192.168.1.4/Donate%20Cash
	GET	91	33w	289c http://192.168.1.4/Planned%20Giving
	GET	91	33w	283c http://192.168.1.4/Site%20Map
	GET	91	33w	289c http://192.168.1.4/Privacy%20Policy
	GET	91	33w	287c http://192.168.1.4/Bequest%20Gift
	GET	91	33w	284c http://192.168.1.4/Gift%20Form
	GET	91	34w	291c http://192.168.1.4/Life%20Income%20Gift
	GET	91	33w	286c http://192.168.1.4/Site%20Assets
404	GET	91	34w	286c http://192.168.1.4/What%20is%20New
Scann	ing: http:	//192.168	.1.4/	
🚨 Ca	ught ctrl+	😋 🚨 saviı	ng scan st	cate to ferox-http_192_168_1_4-1723366593.state
Scann	ing: http:	//192.168	.1.4/	
Scann	ing: http:	//192.168	.1.4/confi	lg/
Scann	ing: http:	//192.168	.1.4/exter	nal/
Scann	ing: http:	//192.168	.1.4/exter	rnal/pnplds/
Scann	ing. http:	//192.100	$\frac{1}{4}/\frac{4}{4}$	//////////////////////////////////////
Scann	ing. neep.	// 192.100	• 1 • 4/ 0003/	
( <b>r</b>	oot⊕kali)	-[~]		
└ <b>─</b> #`f	eroxbuster	-u http:/	//192.168.	.1.4 -q -S 285,286,283,289 -
403	GET	11l	32w	-c Auto-filtering found 404-like response and
	GET	91	32w	-c Auto-filtering found 404-like response and
302	GET	01	0w	0c http://192.168.1.4/ ⇒ login.php
301	GET	91	28w	$309c \text{ http://192.168.1.4/docs} \Rightarrow \text{http://192.168}$
301	GET	91	28w	311c http://192.168.1.4/config ⇒ http://192.16
200	GET	11	10w	105c http://192.168.1.4/docs/pdf.html
200	GET	471	282w	1864c http://192.168.1.4/config/config.inc.php.
200	GEI	4/1	282w	1859c http://192.168.1.4/config/config.inc.php.
200	GEI	01	0W 2.0	0c nttp://192.168.1.4/config/config.inc.pnp
301 201	GET	91	28W	313C  http://192.168.1.4/external   http://192
200	GET	9L 01	20W	$324c \operatorname{Http:}//192.100.1.4/external/php105/0.0 \Rightarrow$
200	GET	91	33W	287c http://192.100.1.4/external/recapiting/reca
404	GET	91	3314	288c http://192.100.1.4/Keports%20List 288c http://192.168 1 4/Style%20Library
	GET	91	34w	290c http://192.168.1.4/neuf%20giga%20nhoto
200	GET	29221	17217w	730335c http://192.168.1.4/docs/DVWA v1.3.ndf
404	GET	91	33w	284c http://192.168.1.4/Home%20Page
404	GET	91	33w	287c http://192.168.1.4/Bequest%20Gift
404	GET	91	33w	284c http://192.168.1.4/Gift%20Form
404	GET	91	34w	291c http://192.168.1.4/Life%20Income%20Gift
Scann	ing. http:	//192 168	1 //	

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
```

[								
	CET	11]	2.2		Auto filtoning found (0			
	GET	01	32W	-c _c	Auto-filtering found 40			
302	GET	01	JZW Øw	-c 0c	http://192.168.1.4/ $\Rightarrow$			
301	GET	91	28w	309c	http://192.168.1.4/docs			
301	GET	91	28w	311c	http://192.168.1.4/conf			
200	GET	11	10w	105c	http://192.168.1.4/docs			
200	GET	47l	282w	1864c	http://192.168.1.4/conf			
301	GET	91	28w	313c	http://192.168.1.4/exte			
301	GET	91	28w	324c	http://192.168.1.4/exte			
200	GET	01	Øw	0c	http://192.168.1.4/exte			
	GET	91	33w	287c	http://192.168.1.4/Repo			
	GET	91	33w	289c	http://192.168.1.4/exte			
404	GET	91	33w	288c	http://192.168.1.4/Styl			
200	GEI	4/l	282W	1859c	http://192.168.1.4/conf			
200	GEI	01	0W 2.4.55	0C	nttp://192.168.1.4/conf			
404		9l 20221	34W 17017w	290C	http://192.168.1.4/neut			
200	GET	2922l 01	1/21/W	7303330	http://192.108.1.4/0000			
	GET	9L 01	33W	2090	http://192.108.1.4/web/ $h$			
	GET	91 91	33w	2860	http://192.108.1.4/My/2			
	GET	91	33w	2840	http://192.168.1.4/Home			
	GET	91	33w	2890	http://192.168.1.4/Plan			
	GET	91	33w	289c	http://192.168.1.4/Pres			
	GET	91	33w	289c	http://192.168.1.4/Priv			
	GET	91	33w	283c	http://192.168.1.4/Site			
	GET	91	33w	284c	http://192.168.1.4/Gift			
	GET	91	33w	285c	http://192.168.1.4/New%			
Scanning	: http://	192.168.	1.4/					
🚨 Caught	t ctrl+c	🚨 savin	g scan st	ate to fe	erox-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/confi	g/				
Scanning	: http://	/192.168.	1.4/exter	nal/				
Scanning	: http://	192.168.	1.4/exter	nal/recap	otcha/			
Scanning	: http://	192.168.	1.4/exter	nal/phpic	ds/			
fero	vhustor -	l∼] u httn•/	/192 168	1 4 - a - k	N 33			
- Tero	vbuster -	-u nccp./	/ 192.100.	1.4 -y -v	v 55 -			
	GET	91	32w	-0	Auto-filtering found 40			
	GET	111	32w	- C	Auto-filtering found 40			
302	GET	01	0w	0c	http://192.168.1.4/ $\Rightarrow$			
301	GET	91	28w	311c	http://192.168.1.4/conf			
301	GET	91	28w	309c	http://192.168.1.4/docs			
200	GET	471	282w	1864c	http://192.168.1.4/conf			
200	GET	47l	282w	1859c	http://192.168.1.4/conf			
200	GET	01	Øw	0c	http://192.168.1.4/conf			
301	GET	91	28w	313c	http://192.168.1.4/exte			
200	GET	Øl	Øw	0c	http://192.168.1.4/exte			
301	GET	91	28w	324c	http://192.168.1.4/exte			
200	GET	11	10w	105c	http://192.168.1.4/docs			
	GET	91	34w	290c	http://192.168.1.4/neuf			
200	GET	29221	17217w	730335c	http://192.168.1.4/docs			
Scanning	: http://	/192.168.	1.4/					
🚨 Caught	t ctrl+c	🚨 savin	g scan st	ate to fe	erox-http_192_168_1_4-17			
Scanning	: http://	192.168.	1.4/	- /				
Scanning	: http://	192.168.	1.4/confi	g/				
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
```

<pre>(root@kali)-[~] # forovbustor _u http://102_168_1_4g</pre>									
	GET	11l	32w	- C	Auto-filteri				
	GET	91	32w	- C	Auto-filteri				
302	GET	01	Øw	0c	http://192.1				
301	GET	91	28w	311c	http://192.1				
301	GET	91	28w	309c	http://192.1				
200	GET	47l	282w	1859c	http://192.1				
200	GET	01	Øw	0c	http://192.1				
301	GET	9l	28w	313c	http://192.1				
200	GET	01	Øw	0c	http://192.1				
	GET	91	33w	287c	http://192.1				
200	GET 29	221	17217w	730335c	http://192.1				
200	GET	1l	10w	105c	http://192.1				
200	GET	47l	282w	1864c	http://192.1				
	GET	9l	33w	288c	http://192.1				
301	GET	91	28w	324c	http://192.1				
	GET	91	34w	290c	http://192.1				
	GET	91	33w	289c	http://192.1				
	GET	9l	33w	285c	http://192.1				
	GET	91	33w	286c	http://192.1				
	GET	91	33w	284c	http://192.1				
	GET	91	33w	289c	http://192.1				
	GET	91	33w	289c	http://192.1				
	GET	91	33w	289c	http://192.1				
	GET	91	33w	283c	http://192.1				
	GET	91	33w	284c	http://192.1				
	GET	91	33w	286c	http://192.1				
Scanning:	http://19	2.168	.1.4/						
Caught	ctrl+c 🚨	savi	ng scan sta	ate to fe	erox-http 192				
Scanning:	http://19	2.168	.1.4/						
Scanning:	http://19	2.168	.1.4/config	<u>z</u> /					
Scanning:	http://19	2.168	.1.4/docs/	, .					
Scanning:	http://19	2.168	.1.4/exterr	nal/					
Scanning:	http://19	2.168	.1.4/exterr	nal/recap	otcha/				
Scanning:	http://19	2.168	.1.4/extern	nal/phpid	ls/				
			,		,				
(root@	<b>⊖ kali</b> )-[~]								
ferox	buster -u	http:	//192.168.1	1.4 -a -N	9				
	GET	91	32w	- C	Auto-filteri				
	GET	111	32w	- C	Auto-filteri				
200	GET	1l	10w	105c	http://192.1				
302	GET	01	Øw	0c	http://192.1				
200	GET 29	221	17217w	730335c	http://192.1				
200	GET	471	282w	1864c	http://192.1				
200	GET	471	282w	1859c	http://192.1				
200	GET	01	Øw	0c	http://192.1				
Scanning:	http://19	2.168	.1.4/						
Scanning:	http://19	2.168	.1.4/docs/						
Scanning:	http://19	2.168	.1.4/config	<u>z</u> /					
Scanning:	http://19	2.168	.1.4/extern	nal/					

# 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
```

└─ <b>#</b> f	eroxbuster	-u http:/	//192.168.	1.4 -q 🚽	<b>—</b>
	GET	91	32w	- c	Auto-filtering found 4(
	GET	11l	32w	- C	Auto-filtering found 40
301	GET	91	28w	309c	http://192.168.1.4/docs
200	GET	11	10w	105c	http://192.168.1.4/docs
301	GET	91	28w	313c	http://192.168.1.4/exte
200	GET	01	Øw	0c	http://192.168.1.4/exte
301	GET	91	28w	324c	http://192.168.1.4/exte
302	GET	01	0w	0c	http://192.168.1.4/ ⇒
	GET	91	33w	287c	http://192.168.1.4/Repo
	GET	91	33w	288c	http://192.168.1.4/Styl
200	GET	471	282w	1859c	http://192.168.1.4/cont
200	GET	01	0w	0c	http://192.168.1.4/cont
301	GEI	91	28w	311c	http://192.168.1.4/coni
200	GEI	4/1	282W	1864c	http://192.168.1.4/coni
200	GEI	29221	1/21/w	/30335c	http://192.168.1.4/docs
	GEI	91	34W	290c	nttp://192.168.1.4/neui
	GEI	91	33W	289c	nttp://192.168.1.4/Web
	GEI	91	33W	2860	nttp://192.168.1.4/Dona
	GET	91	33W	284C	nttp://192.168.1.4/Home
	GET	91	33W	2890	nttp://192.168.1.4/Pr1
	GET	91	33W	2890	nttp://192.168.1.4/Pres
	GET	91	33W	2830	http://192.168.1.4/SIL
		91	2.5W	2040	http://192.100.1.4/011
	GET	91	24W	2910	http://192.100.1.4/LITE
	GET	9L 01	33W	2850	http://192.100.1.4/New/
Scann	ing, http:	//192 168	1 4/	2000	100.1.4/510
Ca	ught ctrl+	//1/2:100:	ig scan st	ate to fe	prox-http 192 168 1 4-1
Scann	ing, http:	//192 168			
Scann	ing. http:	//192.168	1.4/docs/		
Scann	ing: http:	//192.168.	1.4/exter	nal/	
Scann	ing: http:	//192.168.	1.4/exter	nal/recar	otcha/
Scann	ing: http:	//192.168.	1.4/exter	nal/phpic	ds/
Scann	ing: http:	//192.168.	1.4/confi	g/	
Scann	ing: http:	//192.168.	1.4/docs/	pdf.html	
Scann	ing: http:	//192.168.	1.4/exter	nal/recap	otcha/recaptchalib.php
Scann	ing: http:	//192.168.	1.4/exter	nal/phpic	1s/0.6
Scann	ing: http:	//192.168.	1.4/confi	g/config.	.inc.php.bak
Scann	ing: http:	//192.168.	1.4/confi	g/config.	.inc.php
Scann	ing: http:	//192.168.	1.4/confi	g/config.	.inc.php.dist
Scann	ing: http:	//192.168.	1.4/docs/	DVWA_v1.3	3.pdf
		-[~]			
└ <b>─#</b> f	eroxbuster	-u http:/	//192.168.	1.4 -q	-filter-status 404 🔫 🗕
		-			
	GET	111	32w	- C	Auto-filtering found 40
404	GET	91	32w	- C	Auto-filtering found 40
301	GET	91	28w	309c	http://192.168.1.4/docs
301	GET	91	28w	311c	http://192.168.1.4/coni
200	GET	11	10w	105c	http://192.168.1.4/docs
302	GEI	0 L	0w	0C	$http://192.168.1.4/ \Rightarrow$
200	GET	4/1	282w	1859c	http://192.168.1.4/coni
301	GEI	91	28w	313c	http://192.168.1.4/exte
200	GEI		0W	0C	http://192.168.1.4/exte
200	GET	4/L	282W	1864C	http://192.168.1.4/Coni
200		9L 20221	28W	324C	http://192.168.1.4/extended bttp://102.168.1.4/extended bttp://102.168.1.4/extended bttp://dec
200	GET	29221	1/21/W	/303350	http://192.168.1.4/docs
Scann	ing: http:	//102 160	1 / /	ØC	102.108.1.4/coni
Scann	ing: http:	//192.108.	$1 \frac{1}{4}$		
Scann	ing: http:	//192.108.	$\frac{1.4}{00cs}$	<u>م (</u>	
Scann	ing. nucp:	// 192.100.	1.4/ 00011	5/	

# 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
```

	<mark>root⊛kali</mark> )- feroxbuster	[~] -u http:,	//192.168.	1.4 -q ┥	F
	GET	91	30141	-0	Auto-filtering found 404-
	GET	111	32w	-c -c	Auto-filtering found 404-
302	GET	01	0w	0 C	http://192.168.1.4/ $\Rightarrow$ 10
301	GET	91	28w	311c	http://192.168.1.4/config
200	GET	471	282w	1864c	http://192.168.1.4/config
200	GET	471	282w	1859c	http://192.168.1.4/config
200	GET	01	0w	0c	http://192.168.1.4/config
301	GET	91	28w	313c	http://192.168.1.4/extern
301	GET	91	28w	324c	http://192.168.1.4/extern
200	GET	01	Øw	0c	http://192.168.1.4/extern
	GET	91	33w	287c	http://192.168.1.4/Report
	GET	91	33w	289c	http://192.168.1.4/extern
301	GET	91	28w	309c	http://192.168.1.4/docs =
200	GET	11	10w	105c	http://192.168.1.4/docs/p
	GET	91	33w	288c	http://192.168.1.4/Style%
	GET	91	33w	285c	http://192.168.1.4/modern
	GET	91	34w	290c	http://192.168.1.4/neuf%2
200	GET	29221	17217w	730335c	http://192.168.1.4/docs/D
	GET	91	33w	285c	http://192.168.1.4/My%20P
	GET	91	33w	285c	http://192.168.1.4/Contac
	GET	91	33w	286c	http://192.168.1.4/Donate
	GET	91	33w	289c	http://192.168.1.4/Press%
	GET	91	33w	283c	http://192.168.1.4/Site%2
	GET	91	33w	289c	http://192.168.1.4/Planne
	GET	91	33w	284c	http://192.168.1.4/Home%2
	GET	91	33w	283c	http://192.168.1.4/About%
404	GET	91	33w	287c	http://192.168.1.4/Beques
Scan	ning: http:/	/192.168	.1.4/		
🪨 (	aught ctrl+c	🧧 🚨 savı	ng scan st	ate to fe	erox-http_192_168_1_4-1/23
Scan	ning: nttp:/	/192.168	.1.4/	~ I	
Scan	ning: nttp:/	/192.100	1.4/CONT1	g/ n n 1 /	
Scan	ning: nttp:/ ning: http:/	/192.100	$\frac{1}{4}$	nal/nocar	atcha/
Scan	ning: nttp:/ ning: http:/	/192.100	$\frac{1}{4}$	nal/recap nal/nhnia	
Scan	ning. http:/	/192.100	$\frac{1}{4} \frac{4}{40}$	πατ/μπρτι	12/
Scan	ning. nccp./	/ 192.100	.1.4/0005/		
	root@kali)-	[~]			
	feroxbuster	_u httn•	//192_168_	1.4 -a	status-codes 200.301
	Teroxbuster	u neep.,	,1)2.100.	±•+ -4	Status - codes 200,501 -
301	GET	91	28w	309c	http://192.168.1.4/docs =
301	GET	91	28w	311c	http://192.168.1.4/config
200	GET	01	0w	0c	http://192.168.1.4/config
200	GET	471	282w	1864c	http://192.168.1.4/config
200	GET	11	10w	105c	http://192.168.1.4/docs/p
200	GET	471	282w	1859c	http://192.168.1.4/config
200	GET	29221	17217w	730335c	http://192.168.1.4/docs/D
301	GET	91	28w	313c	http://192.168.1.4/extern
301	GET	91	28w	324c	http://192.168.1.4/extern
200	GET	01	0w	0c	http://192.168.1.4/extern
Scan	ning: http:/	/192.168	.1.4/		1
Scan	ning: http:/	/192.168	.1.4/confi	g/	
Scan	ning: http:/	/192.168	.1.4/docs/		
Scan	ning: http:/	/192.168	.1.4/exter	nal/	
Scan	ning: http:/	/192.168	.1.4/exter	nal/phpic	ls/
Scan	ning: http:/	/192.168	.1.4/exter	nal/recap	otcha/

# **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

	( <b>root®kali</b> )-[~] -# feroxbuster -u http://192.168.1.4 -Aburp										
I I by B	)    \ en "epi" Ri	)  _\ isher	/ _ `   ∖, ≌	/_\ \_/	\_/   / \   	  _ er:	_	 • 4			
6	Target Url	L		http:/	//192.3	168	.1.4				
1	Threads			50 /////////	hana /	~~~	licto				lah Cant
A	Status Coc	des		All St	atus (	Cod	es!	/ DT2(	Jove	ry/w	eb-conc
<u>ж</u>	Timeout (s	secs)		7							
<b>49</b>	User-Agent	t		Random							-
*	Config Fil	le		/etc/f	eroxb	ust	er/fe	rox-0	conf	ig.t	oml
	Froxy Extract Li	inks		true	/ 12/ •	0.0	.1.00	00			
<b>p</b> 886	HTTP metho	ods		[GET]							
-	Insecure			true							
t)	Recursion	Depth	h	4							
<b>p</b> \$\$\$	Press [EN]	TER] 1	to use th	ne Scan	Manag	eme	nt Me	nu™			·
	GET		9l	32w		- C	Auto-	filte filte	erin	g fo	und 404
	GET	-	LIL	32W	•	- C	AULO-	τιιι	srin	IS TO	una 404
302	GET		Ø1	Øw	(	٥c	httn·	//193	) 16	8 1	$4/ \Rightarrow 1$
302 301	GET GET		0l 9l	0w 28w	31:	0c 1c	http: http:	//192 //192	2.16 2.16	8.1.	4/ ⇒ l 4/confi
302 301 \$	GET GET		01 91	0w 28w	31: 	0C 1C Burp Su	http: http: <sup>ite Community</sup>	// 192 // 192 y Edition v20	2.16 2.16	8.1. 8.1. Temporary	4/ ⇒ l 4/confi Project
302 301 S Burp Pri Dashboa	GET GET oject Intruder Repeater rd Target Proxy	· View He Intruder	Øl 9l elp Repeater C	Øw 28w	31: E guencer E	0 C 1 C Burp Su Decoder	http: http: ite Community	// 192 // 192 y Edition v20	2 . 16 2 . 16 024.5.5 - <sup>-</sup>	8.1. 8.1. Temporary	4/ ⇒ l 4/confi Project
302 301 Burp Pr Dashboa Intercept	GET GET oject Intruder Repeater rd Target <u>Proxy</u> t <u>HTTP history</u> We	· View He Intruder 2bSockets hist	01 91 elp Repeater Cr tory Ø Proxy	Øw 28w ollaborator See settings	31: F	0 C 1 C Burp Su Decoder	http: http: ite Community	// 192 // 192 y Edition v20	2 . 16 2 . 16 024.5.5 - <sup></sup> Iger	8.1. 8.1. Temporary Organizer	4/ ⇒ l 4/confi Project Extensions
302 301 S Burp Pr Dashboa Intercept	GET GET	View He Intruder bSockets hist e and general	01 91 Repeater Critory @ Proxy L binary content	Øw 28w ollaborator See settings	quencer E	0 C 1 C Burp Su Decoder	http: http: iteCommunity Compar	// 192 // 192 y Edition v20 rer Log	2.16 2.16 024.5.5 - 1 1ger	8.1. 8.1. Temporary Organizer	4/ ⇒ l 4/confi Project Extensions
302 301 S Burp Pr Dashboa Intercept T Filter # ^ Hos 1 htt	GET GET	View He Intruder bSockets hist and general Method U GET Ir	01 91 Repeater Co tory © Proxy L binary content IRL repos/epi052/feroxbus	Øw 28w ollaborator See settings ster/releases	quencer C ams Edited	0 C 1 C Burp Su Decoder Statu 200	http: http: iteCommunit r Compar us code Ler 26:	// 192 // 192 y Edition v20 rer Log ngth MIM 394 JSON	2 • 16 2 • 16 024.5.5 Iger E type E	8.1. 8.1. Temporary Organizer	4/ ⇒ l 4/confi Project Extensions
302 301 Surp Pr. Dashboa Intercept V Fitter # ^ Hor 1 htt 2 htt 3 htt	GET GET	View He Intruder bSockets hist and general Method U GET /r GET / GET /r	01 91 Repeater Critory CProxy L binary content RL repos/epi052/feroxbus robots.txt	0w 28w ollaborator See settings ster/releases	quencer C ams Edited	0 C 1 C Burp Su Decoder Statu 200 302 200	http: http: iteCommunity r Compar uscode Ler 26: 479 309	// 192 // 192 y Edition v20 rer Loc ngth MIM 394 JSOP 9 HTM 9 text	2 • 16 2 • 16 2 • 16 024.5.5 Iger Iger E type E N L	8.1. 8.1. Temporary Organizer Extension	4/ ⇒ 1 4/confi Project Extensions
302 301 5 Burp Pr Dashboa Intercept 7 Filter # ^ Hor 1 htt 2 htt 3 htt 4 htt 5 htt	GET GET	View He Intruder Sockets hist and general Method U GET /r GET / GET / GET / GET /	01 91 Repeater Co tory © Proxy L binary content RL repos/epi052/feroxbus robots.txt	0w 28w ollaborator See settings ster/releases	quencer C arms Edited	0 C 1 C 3urp Su Decoder Statu 200 302 200 302 404	http: http: ite Community r Comparing us code Ler 263 476 300 477 300 587	// 192 // 192 y Edition v20 rer Log rer Log http:// 2016 8394 JSOP 9 HTM 9 HTM 9 HTM 7 HTM	2 • 16 2 • 16 024.5.5 - Iger E type E N L L L	8.1. 8.1. Temporary Organizer	4/ ⇒ 1 4/confi Project Extensions Title
302 301 5 Burp Pr Dashboa Intercept ♥ Fitter # ∧ Hos 1 htt 2 htt 4 htt 5 htt 6 htt 7 htt	GET GET oject Intruder Repeater rd Target Proxy t HTTP history We r settings: Hiding CSS, image st p://api.github.com p://192.168.1.4 p://192.168.1.4 p://192.168.1.4 p://192.168.1.4 p://192.168.1.4	View He Intruder bSockets hist and general Method U GET /r GET /r GET / GET / GET / GET / GET /	01 91 Repeater Critical tory 0 Proxy l binary content IRL repos/epi052/feroxbus robots.txt e1934804561a4fab9e htaccess13f862d2fbb	Øw 28w	quencer E ams Edited	0 C 1 C 3urp Su Decoder Statu 200 302 200 302 403	http: http: ite Communit r Compar us code Ler 263 475 309 478 583 600 544	// 192 // 192 y Edition v20 rer Log rer Log http:// Log by JSOP by HTM by text 3 HTM 7 HTM 7 HTM 3 HTM 4 HTM	2 • 16 2 • 16 024.5.5	8.1. 8.1. Temporary Organizer Extension	4/ ⇒ 1 4/confi Project Extensions Title 404 Not Found 403 Forbidden 403 Forbidden
302 301 Burp Pr Dashboa Intercept ♥ Filter # ^ Hos 1 htt 2 htt 3 htt 4 htt 5 htt 6 htt 8 htt	GET GET           oject         Intruder         Repeater           rd         Target         Proxy           rd         HTTP history         We           r settings: Hiding CSS, image         st           ps://api.github.com         p://192.168.1.4           p://192.168.1.4         p://192.168.1.4           p://192.168.1.4         p://192.168.1.4           p://192.168.1.4         p://192.168.1.4	View He Intruder bSockets hist and general Method U GET /r GET /r GET /r GET /f GET /A GET /A GET /A	0 9 9 Repeater Cri tory 0 Proxy I binary content RL repos/epi052/feroxbus robots.txt e193d804561a4fab9e htaccess13f862d2fbb htaccess13f862d2fbb	0w 28w ollaborator see settings ster/releases eaf95ead23a 84794816b 21476fa1f4b5 447c6b437c0	quencer C ams Edited	0 C 1 C 3 urp Su 0 c 3 urp Su 0 c 0 c 0 c 1 c 1 c 1 c 1 c 1 c 1 c 1 c 1	http: http: ite Community r Compare us code Ler 263 479 309 478 587 600 544 525	// 192 // 192 y Edition v2( rer Loc erer Hor erer Hor Hor Hor Hor Hor Hor Hor Hor Hor Hor	2 • 16 2 • 16 1	8.1. 8.1. Temporary Organizer Extension	4/ ⇒ 1 4/confi Project Extensions Title 404 Not Found 403 Forbidden 404 Not Found
302 301 5 Burp Pr Dashboa Intercept 7 Filter # ^ Hos 1 htt 2 htt 3 htt 4 htt 5 htt 6 htt 7 htt 8 htt 9 htt 10 htt	GET GET	View He Intruder Sockets hist and general Method U GET /r GET / GET / GET /I GET /I GET /I GET /a GET /a GET /ii	01 91 Repeater Co tory 0 Proxy l binary content RL epos/epi052/feroxbus robots.txt e193d804561a4fab9e htaccess13f862d2fbb htaccessacebbd73112 admin3b55834e5bed admin07fdd621ed874 mages	0w 28w ollaborator See settings ster/releases eaf95ead23a 84794816b 21476fa1f4b5 217c6b437c0 1491988f38	quencer C ams Edited	0 C 1 C 3 Jurp Su Decoder 200 302 200 302 404 403 403 404 404	http: http: ite Community r Comparison us code Ler 263 479 306 478 587 587 587 587 587 587 587 587 587 5	// 192 // 192 y Edition v20 rer Log rer Log httm 394 JSOP 9 HTM 394 HTM 394 HTM 394 HTM 40 HTM 40 HTM 40 HTM 40 HTM 7 HTM	2 • 16 2 • 16 1	8.1. 8.1. Temporary Organizer Extension	4/ ⇒ 1 4/confi Project Extensions Title 404 Not Found 403 Forbidden 403 Forbidden 404 Not Found 404 Not Found 404 Not Found
302 301 Surp Pr Dashboa Intercept ¥ ^ Hor 1 htt 2 htt 3 htt 4 htt 5 htt 6 htt 7 htt 8 htt 9 htt 10 htt 11 htt 2 htt 1 htt 1 htt 2 htt 1 htt 1 htt 2 htt 1 htt 1 htt 1 htt 2 htt 1 htt 1 htt 2 htt 1 htt 1 htt 2 htt 1 htt 1 htt 2 htt 1 htt 1 htt 1 htt 2 htt 1 httt 1 htt 1 httt 1 htt 1 httt 1 httt 1 httt 1 httt 1 ht	GET GET oject Intruder Repeater rd Target Proxy t HTTP history We r settings: Hiding CSS, image st ps://api.github.com p://192.168.1.4 p://192.168.1.4 p://192.168.1.4 p://192.168.1.4 p://192.168.1.4 p://192.168.1.4 p://192.168.1.4 p://192.168.1.4 p://192.168.1.4 p://192.168.1.4	View He Intruder Sockets hist and general Method U GET /r GET / GET / GET /I GET /I GET /a GET /a GET /in GET /in GET /in GET /in	01 91 Repeater Criteria Criter	Øw 28w	quencer C ams Edited	0 C 1 C 3 Jurp Su 0 De coder 2000 302 2000 302 404 403 403 404 404 404 404	http: http: ite Communit r Compar us code Ler 265 479 309 478 587 600 544 592 491 491 491	// 192 // 192 y Edition v20 rer Log rer Log http:// 192 y Edition v20 rer Log http:// 192 http:// 192	2 • 16 2 • 16 1	8.1. 8.1. Temporary Organizer Extension xt	4/ ⇒ 1 4/confi Project Extensions Title 404 Not Found 403 Forbidden 404 Not Found 404 Not Found 404 Not Found 404 Not Found
302 301 Burp Pr Dashboa Intercept ♥ Fitter # ^ Hor 1 htt 3 htt 4 htt 5 htt 6 htt 7 htt 8 htt 9 htt 10 htt 11 htt 2 htt 2 htt	GET GET oject Intruder Repeater rd Target Proxy t HTTP history We r settings: Hiding CSS, image st ps://api.github.com p://192.168.1.4 p://192.168.1.4 p://192.168.1.4 p://192.168.1.4 p://192.168.1.4 p://192.168.1.4 p://192.168.1.4 p://192.168.1.4	View He Intruder bSockets hist and general Method U GET /r GET /r GET /r GET / GET / GET /a GET /a GET /a GET /in GET /s GET /in	01 91 Repeater Critory © Proxy I binary content RL repos/epi052/feroxbus robots.txt e1934804561a4fab9e htaccess13f862d2fbb htaccess13f862d2fbb htaccess13f862d2fbb htaccess13f862d2fbb htaccess13f862d2fbb htaccess13f862d2fbb	0w 28w ollaborator set settings ster/releases eaf95ead23a 84794816b e1476fa1f4b5 47c6b437c0 4491988f38	quencer E ams Edited	0 C 1 C 3 urp Su Decoder 200 302 200 302 200 302 200 302 404 403 404 404 404 404	http: http: ite Communit r Compar us code Ler 263 476 306 476 587 600 544 529 597 491 494	// 192 // 192 y Edition v20 rer Log rer Log mgth MIM 394 JGN 9 text 3 HTM 9 HTM 8 HTM 7 HTM 8 HTM 9 HTM 9 HTM 9 HTM 9 HTM 9 HTM 9 HTM 9 HTM 9 HTM	2 . 16 2 . 17 2	8.1. 8.1. Temporary Organizer Extension xt	4/ ⇒ 1 4/confi Project Extensions Title 404 Not Found 403 Forbidden 404 Not Found 404 Not Found 404 Not Found 404 Not Found 404 Not Found
302 301 Burp Pr Dashboa Intercept ▼ Filter # ^ Hor 1 htt 2 htt 3 htt 4 htt 5 htt 6 htt 7 htt 8 htt 10 htt 11 htt 2 htt 3 htt 4 htt 5 htt 6 htt 7 htt 8 htt 10	GET GET oject Intruder Repeater rd Target Proxy t HTTP history We r settings: Hiding CSS, image st ps://api.github.com p://192.168.1.4 p://192.168.1.4 p://192.168.1.4 p://192.168.1.4 p://192.168.1.4 p://192.168.1.4 p://192.168.1.4 p://192.168.1.4 p://192.168.1.4	View He Intruder Sockets hist and general Method U GET /r GET / GET / GET /I GET /I	01 91 Repeater Co tory © Proxy L binary content RL epos/epi052/feroxbus robots.txt e193d804561a4fab9e htaccess13f862d2fbb htaccess13f864d2fbbb htaccess14fbbbb htaccess14fbbbb htaccess14f	Ow 28w	quencer C ams Edited	0 C 1 C 3 Jurp Su 200 302 200 302 200 302 404 403 403 404 404 404 404 8 Kes	http: http: ite Community r Compar us code Ler 265 479 309 476 587 600 544 522 497 499 499 499	// 192 // 192 y Edition v20 rer Log rer Log htm 994 JSON 9 HTM 994 HTM 994 HTM 7 HTM 7 HTM 7 HTM 7 HTM 7 HTM 7 HTM 7 HTM	2 • 16 2 • 16 1	8.1. 8.1. Temporary Organizer Extension xt	4/ ⇒ 1 4/confi Project Extensions Title 404 Not Found 403 Forbidden 404 Not Found 404 Not Found 404 Not Found 404 Not Found 404 Not Found
302 301 Burp Pr Dashboa Intercept ♥ Fitter # ^ Ho; 1 htt 2 htt 3 htt 4 htt 5 htt 6 htt 7 htt 10 htt 11 htt 12 htt 12 htt 8 htt 9 htt 11 htt 9 htt 11 htt 9 htt 11 htt 9 htt 12 htt 9 htt 11 htt 9 htt 11 htt 9 htt 12 htt 9 htt 11 htt 9 htt 11 htt 9 htt 12 htt 9 htt 12 htt 9 htt 11 htt 9 htt 12 htt 9 htt 12 htt 9 htt 11 htt 12 htt 11 htt 9 htt 11 htt 11 htt 9 htt 11 htt 11 htt 9 htt 11 htt 9 htt 11 htt 9 htt 11 htt 12 htt 11 htt 12 htt 11 htt 12 htt 11 htt	GET GET           oject         Intruder         Repeater           rd         Target         Proxy           t         HTTP history         We           r settings: Hiding CSS, image         st           ps://api.github.com         p://192.168.1.4           p://192.168.1.4         p://192.168.1.4	View He Intruder bSockets hist and general Method U GET /r GET /r GET // GET /i GET /a GET /a GET /i GET /s GET /s GET /r	01 91 Repeater Critical Content tory 0 Proxy I binary content IRL repos/epi052/feroxbus robots.txt e193d804561a4fab9e htaccess13f862d2fbb htaccess13f862d2fbb htaccessacebbd73112 admin3b55834e5bed admin07fdd621ed874 mages sites mg	Ow 28w ollaborator Sec settings Para ster/releases Para ster/re	quencer E ams Edited	0 C 1 C 30 urp Su 0 c 30 urp Su 0 c 0 d 0 d 0 d 0 d 0 d 0 d 0 d 0 d	http: http: ite Communit r Compar us code Ler 263 479 300 478 588 600 544 549 490 490 490 490 490 490 490 490 490	// 192 // 192 y Edition v20 rer Log rer Log re	2 • 16 2 • 16 1	8.1. 8.1. Temporary Organizer Extension xt	4/ ⇒ 1 4/confi Project Extensions Title 404 Not Found 403 Forbidden 403 Forbidden 404 Not Found 404 Not Found 404 Not Found 404 Not Found 404 Not Found
302 301 Burp Pr Dashboa Intercept ▼ Filten # ^ Hos 1 htt 2 htt 3 htt 4 htt 5 htt 6 htt 7 htt 8 htt 9 htt 10 htt 11 htt 2 htt 8 htt 9 htt 10 htt 12 htt 2 htt 10 htt 11 htt 2 htt 10 htt 11 htt 2 htt 10 htt 11 htt 2 htt 10 htt 11 htt 2 htt 10 htt 10 htt 11 htt 2 htt 10 htt 11 htt 2 htt 10 htt 10 htt 11 htt 2 htt 10 htt 12 htt 10 htt 12 htt 10 htt 11 htt 2 htt 10 htt 11 htt 2 htt 10 htt 12 htt 10 htt 11 htt 2 htt	GET GET           oject         Intruder         Repeater           rd         Target         Proxy           t         HTTP history         We           r settings: Hiding CSS, image         st           ps://api.github.com         p://92.168.1.4           p://92.168.1.4         p://92.168.1.4           p://92.168.1.4         p://92.168.1.4           p://92.168.1.4         p://92.168.1.4           p://92.168.1.4         p://92.168.1.4           p://92.168.1.4         p://92.168.1.4           p://92.168.1.4         p://92.168.1.4           p://192.168.1.4         p://92.168.1.4	View He Intruder bSockets hist and general Method U GET /r GET / GET / GET /I GET /I G	0 9 Repeater Co Repeater Co tory © Proxy L binary content RL repos/epi052/feroxbus robots.txt e193d804561a4fab9e htaccess13f862d2fbb htaccess13f862d2fbb htaccessacebbd73112 admin07fdd621ed874 mages sites mg	Ow 28w	ams Edited	0 C 1 C 3 urp Su becoder 200 302 200 302 200 302 404 403 403 404 404 404 404 404	http: http: ite Community r Compare us code Ler 263 477 300 263 477 477 300 263 477 477 477 477 477 477 477 477 477 47	// 192 // 192 y Edition v2( rer Log rer HTM rer HTM re	2 • 16 2 • 16 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	8.1. 8.1. Temporary Organizer Extension xt	4/ ⇒ 1 4/confi Project Extensions Title 404 Not Found 403 Forbidden 403 Forbidden 404 Not Found 404 Not Found 404 Not Found 404 Not Found 404 Not Found 404 Not Found
302 301 Burp Pr Dashboa Intercept ▼ Filter # ^ Hor 1 htt 2 htt 3 htt 4 htt 5 htt 6 htt 7 htt 8 htt 10 htt 11 htt 2 htt 3 htt 2 htt 3 htt 3 htt 2 htt 3 htt 3 htt 1 GET 2 User 1 GET 2 User 3 Acce	GET GET oject Intruder Repeater rd Target Proxy t HTTP history We r settings: Hiding CSS, image st p://api.dist.uk p://api.dis	View He Intruder bSockets hist and general Method U GET /r GET /r GET // GET /i GET /i GET /i GET /i GET /i GET /s GET /s GET /s GET /i GET /s GET /s GET /s GET /s GET /s	01 91 Repeater Criteria Content tory © Proxy tbinary content RL repos/epi052/feroxbus robots.txt e193d804561a4fab9e htaccess13f86242fbb htaccess13f8624fbb htaccess13f8624fbb htaccess13f8624fbb htaccess13f8624fbb htaccess13f862fb htaccess1	Ow 28w	ams Edited	0 C 1 C 3 urp Su ve coder Statu 200 302 404 403 403 404 404 404 404 404	http: http: ite Communit r Compar us code Ler 263 479 300 544 587 600 544 592 499 490 490 490 490 490 490 490 490 490	//192 //192 y Edition v20 rer Log rer Log rer Log rer Log http: y Edition v20 http: y Edition v20 http: http	2 • 16 2 • 16 1	8.1. 8.1. Temporary Organizer Extension xt	4/ ⇒ 1 4/confi Project Extensions Title 404 Not Found 403 Forbidden 403 Forbidden 404 Not Found 404 Not Found 405 Found 406 Not Found 406 Not Found 406 Not Found 407 Found 408 Not Found 408 Not Found 408 Not Found 409 Not Found 409 Not Found 400 Not Found
302 301 Burp Pr Dashboa Intercept ♥ Filter # ^ Host 1 htt 2 htt 3 htt 4 htt 5 htt 6 htt 10 htt 11 htt 2 htt 12 htt 12 htt 2 htt 13 htt 4 htt 5 htt 6 htt 10 htt 11 htt 2 htt 12 htt 13 htt 14 htt 5 htt 6 htt 10 htt 11 htt 2 htt 12 htt 12 htt 13 htt 14 htt 5 htt 6 htt 10 htt 11 htt 2 htt 12 htt 13 htt 14 htt 15 htt 6 htt 10 htt 11 htt 2 htt 12 htt 12 htt 13 htt 14 htt 15 htt 16 htt 17 htt 18 htt 10 htt 11 htt 12 htt 10 htt 11 htt 12 htt 13 htt 14 htt 15 htt 16 htt 11 htt 12 htt 10 htt 11 htt 12 htt 13 htt 14 htt 15 htt 16 htt 11 htt 12 htt 16 htt 11 htt 12 htt 16 htt 17 htt 18 htt 18 htt 19 htt 10 htt 11 htt 12 htt 10 htt 11 htt 12 htt 11 htt 12 htt 11 htt 12 htt 14 htt 15 htt 16 htt 11 htt 17 htt 16 htt 11 htt 17 htt 18 htt	GET GET oject Intruder Repeater rd Target Proxy t HTTP history We r settings: Hiding CSS, image st ps://api.github.com py//192.168.1.4 py//192.168.1.4 py//192.168.1.4 py//192.168.1.4 py//192.168.1.4 py//192.168.1.4 py//192.168.1.4 py//192.168.1.4 py//192.168.1.4 py//192.168.1.4 py//192.168.1.4 py//192.168.1.4 py//192.168.1.4 py/192.168.1.4 py/192.168.1.4 py/192.168.1.4 py/192.168.1.4	View He Intruder bSockets hist and general Method U GET /r GET /r GET / GET /I GET /A GET /A	0 9 Repeater Co tory © Proxy binary content RL repos/epi052/feroxbus robots.txt e193d804561a4fab9e htaccess13f862d2fbb htaccessacebbd73112 admin07fdd621ed874 mages sites mg 4b57451a08dcb ⊢ NT 6.1; W0W64) 2526.111 Safari /	Ow 28w	31: quencer C ams Edited	0 C 1 C Surp Su Decoder Statt 200 302 200 302 200 302 404 404 404 404 404 404 404 4	http: http: ite Communit r Compar r Compar compar r Compar compar compar compar compar compar compar compar compar compar compar compar compar compar compar	//192 //192 y Edition v2( rer Log erer Log agth MIM 394 JSOP 0 HTM 394	2 . 16 2 . 16 2 . 16 2 . 16 2 . 16 2 . 16 2 . 16 16 16 16 16 16 16 16 16 16 16 16 16 1	8.1. 8.1. Temporary Organizer Extension xt	4/ ⇒ 1 4/ confi Project Extensions Title 404 Not Found 403 Forbidden 403 Forbidden 404 Not Found 404 Not Found
302 301 Burp Pr Dashboa Intercept ▼ Filter # ^ Hor 1 htt 2 htt 3 htt 4 htt 5 htt 6 htt 7 htt 8 htt 10 htt 11 htt 2 htt 3 ht	GET GET oject Intruder Repeater rd Target Proxy t HTTP history We rsettings: Hiding CSS, image st ps://api.github.com p//192.168.1.4 pp//192.168.1.4 pp//192.168.1.4 pp//192.168.1.4 pp//192.168.1.4 pp//192.168.1.4 pp//192.168.1.4 pp//192.168.1.4 pp//192.168.1.4 pp//192.168.1.4 pp//192.168.1.4 pp//192.168.1.4 pp:/192.168.1.4 pp:/192.168.1.4 ection: keep-alive	View He Intruder bSockets hist and general Method U GET /r GET /r GET // GET /i GET /i	0 9 elp Repeater Cri tory   ② Proxy tbinary content IRL repos/epi052/feroxbus robots.txt e193d804561a4fab9e htaccess13f862d2fbb htaccess13f862d2fbb htaccess13f862d2fbb htaccess3acebbd73112 admin3b55834c5bed admin07fdd621ed874 mages sites mg 4b57451a08dcb ⊢ NT 6.1; W0W64) 2526.111 Safari/	Øw 28w	ams Edited	0 C 1 C 3 urp Su 200 302 404 403 403 403 404 404 404 404	http: http: ite Communit r Compar us code Ler 263 479 300 544 587 600 544 587 600 544 587 600 544 587 600 544 587 600 544 587 600 544 592 499 499 499 499 499 499 499 499 499 4	//192 //192 y Edition v20 rer Log rer Log rer Log http://www. gath MIM 99 http://www. 39 http://www. 30 http://wwww. 30 http://wwww. 30 http://www. 30 http:	2.16 2.16 2.16 2.4.5.5. ger Etype E L L L L L L L L L L L L L L L L L L L	8.1. 8.1. Temporary Organizer Extension xt extension xt	4/ ⇒ 1 4/ confi Project Extensions Title 404 Not Found 403 Forbidden 403 Forbidden 404 Not Found 404 Not Found 405 Found 406 Not Found 406 Not Found 407 Found 408 Not Found 408 Not Found 408 Not Found 409 Not Found 409 Not Found 400 Not Foun
3 0 2 3 0 1 Burp Pr Dashboa Intercept ♥ Filten # ^ Hos 1 htt 2 htt 3 htt 4 htt 5 htt 6 htt 7 htt 8 htt 9 htt 10 htt 2 htt 2 htt 1 htt 2 htt 3 htt 4 htt 5 htt 6 htt 1 htt 2 htt 1 htt 2 htt 3 htt 1 htt 2 htt 3 htt 4 htt 5 htt 6 htt 1 htt 2 htt 1 htt 2 htt 3 htt 1 htt 2 htt 5 htt 6 htt 1 htt 2 htt 1 htt 2 htt 3 htt 1 htt 2 htt 1 htt 1 htt 2 htt 1 htt 1 htt 1 htt 1 htt 2 htt 1	GET GET oject Intruder Repeater rd Target Proxy t HTTP history We r settings: Hiding CSS, image st ps://api.github.com pj/192.168.1.4 pj/192.168.1.4 pj/192.168.1.4 pj/192.168.1.4 pj/192.168.1.4 pj/192.168.1.4 pj/192.168.1.4 pj/192.168.1.4 pj/192.168.1.4 pj/192.168.1.4 pj/192.168.1.4 pj/192.168.1.4 pj/192.168.1.4 pj. Like Gecko) Chrco pt: */* : 192.168.1.4 ection: keep-alive	View He Intruder Sockets hist and general Method U GET /r GET / GET /I GET /I G	01 91 Repeater Co tory © Proxy L binary content RL repos/epi052/feroxbus robots.txt e193d804561a4fab96 htaccess13f862d2fbb htaccessacebbd73112 admin355834e5bed admin355834e5bed admin355834e5bed admin355834e5bed admin355834e5bed sites mg	0w 28w	311: quencer □ ams Edited	0 C 1 C 3 urp Su 200 302 200 302 200 302 404 403 403 404 404 404 404 404	http: http: ite Community r Compare us code Ler 265 479 309 478 587 600 544 587 600 544 587 600 544 587 600 544 587 600 544 587 600 544 587 600 544 587 600 544 587 600 544 592 497 499 499 499 499 499 499 499 499 499	//192 //192 y Edition v20 rer Log rer Log rer Log hTM 394 JSON 9 HTM 394 JSON 9 HTM 394 JSON 9 HTM 394 JSON 9 HTM 394 JSON 9 HTM 394 JSON 9 HTM 394 JSON 394	2.16 2.16 2.16 2.16 2.16 2.16 2.16 10 10 10 10 10 10 10 10 10 10 10 10 10	8.1. 8.1. Temporary Organizer Extension xt extension xt extension xt	<pre>4/ ⇒ l 4/confi Project Extensions Title 404 Not Found 403 Forbidden 403 Forbidden 404 Not Found Extensions GMT =iso-8859-1 DTD HTML 2.0//</pre>

# **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( ferox	<mark>8 kali</mark> ) (buster	-[ <b>~</b> ] -u http	://19	92.168.	1.4 -m P(	DST 🔫	
   by B	   en "e	) _   _) _   \ epi" Ri	)   /  )   /   \   \	— 、 ,		\_/     / \     ver	/   /   : 2.10.4	
6	Targ	get Url			http:	//192.168	3.1.4	
27	Word	aus 11ict			- 20 /115 m/	sharo/so	-lists/D	iscovery/Web-Con
Ā	Wordlist Status Codes				tatus Co	les!	ISCOVELY/WED CON	
¥	Time	eout (s	ecs)		7			
<del>69</del>	User	-Agent			ferox	buster/2	.10.4	
. A	Conf	<sup>:</sup> ig Fil	.e		/etc/	feroxbust	ter/fero	x-config.toml
<i>,</i>	Extr	act Li	.nks		true	_		
<b>P</b> 88	HTTF	o methc	ods		LPOST	j		
	Reci	irsion	Depth		4			
<b>p</b> 888	Pres	s [ENT	ER] to u	se th	ie Scan	Manageme	ent Menu	тм
404	F	POST	91		32w	- c	Auto-fi	ltering found 40
403	F	POST	11l		32w	- C	Auto-fi	ltering found 40
302	F	POST	0l		Øw	0c	http://	192.168.1.4/ ⇒
301	F	POST	91		28w	309c	http://	192.168.1.4/docs
200		GET	1l		10w	105c	http://	192.168.1.4/docs
301	F	POST	91		28w	313c	http://	192.168.1.4/exte
200		GET	01		0w	0c	http://	192.168.1.4/exte
301		GET	91		28w	324c	http://	192.168.1.4/exte
404		GEI	9l		32w	302c	http://	192.168.1.4/exte
404	F	GEI	91		32W	299C	nttp://	192.168.1.4/exte
200	٢	2051 GET	9L 20221	1 7	33W 7217w	20/C	nttp://	192.108.1.4/Repo
200			2922l 01	1/	23W 71/W	7303330	http://	192.100.1.4/0005
404 301	r C		91 01		22₩ 28₩	200C 311c	httn•//	192.100.1.4/Styl
200	F	GET	01		20w	0C	httn·//	192.168.1.4/conf
200		GET	471		282w	1864c	http://	192.168.1.4/conf
404	P	POST	91		33w	2850	http://	192.168.1.4/mode
404	F	POST	91		34w	290c	http://	192.168.1.4/neuf
200		GET	471		282w	1859c	http://	192.168.1.4/conf
404	F	POST	91		33w	285c	http://	192.168.1.4/Cont
404	F	POST	91		33w	286c	http://	192.168.1.4/Dona
404	P	POST	91		33w	284c	http://	192.168.1.4/Home
404	F	POST	91		33w	289c	http://	192.168.1.4/Plan
404	F	POST	91		33w	289c	http://	192.168.1.4/Pres
404	F	POST	91		33w	289c	http://	192.168.1.4/Priv
404	F	POST	91		33w	283c	http://	192.168.1.4/Site
404	P	POST	91		33w	284c	http://	192.168.1.4/Gift
404	P	POST	91		34w	291c	http://	192.168.1.4/Life
404	P	POST	91		33w	285c	http://	192.168.1.4/New%
404	F	POST	91		33w	286c	http://	192.168.1.4/Site
####			<del>          </del>	- 4s	29	991/30014	+ 0s	tound: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

<b>_</b> #	-( <b>root®kali</b> ) feroxbuster	)-[~] u http:/	/192.168.1.4	-H 'Cont	ent-Type:	applicatio	on/x-www-fo	rm-urlencod	ed'burp -c		
404 403 302 301 200 200 200 301 301	GET GET GET GET GET GET GET GET GET	91 111 91 91 471 01 471 91 91	32w 32w 0w 28w 28w 282w 0w 282w 282w 28w 28w	-c Aut -c Aut 0c htt 309c htt 311c htt 1859c htt 0c htt 1864c htt 313c htt 324c htt	o-filteri o-filteri p://192.1 p://192.1 p://192.1 p://192.1 p://192.1 p://192.1 p://192.1 p://192.1	ng found 40 $(68.1.4) \Rightarrow$ $(68.1.4) \Rightarrow$ (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) < (68.1.4) <	04-like resp 04-like resp 10gin.php s ⇒ http:// fig ⇒ http fig/config.: fig/config.: prnal ⇒ htt ernal/phpta ernal/precap	<pre>conse and c: conse and c: /192.168.1 ://192.168.1 inc.php.bak inc.php.dis inc.php.dis tp://192.166 s/0.6 ⇒ ht tc.ba/recant</pre>	reated new fi reated new fi 4/docs/ 1.4/config/ t 8.1.4/externa tp://192.168. chalib php	lter; tog lter; tog l/ 1.4/exter	gl
S Burn	Project Intruder R	Repeater View He		Burp Suite Com	munity Edition v2024.5.	5 - Temporary Project	· · · · · · · · · · · · · · · · · · ·			008	
Dasi Inte	hboard Target P rcept HTTP history	Proxy Intruder WebSockets his	Repeater Collabo story   🚯 Proxy set	orator Sequen ttings		Comparer Log	gger Organizer			Settings	
T F	Filter settings: Hiding C	 SS, image and gene								0:	
# ~ 1 1 1 1 1 1 1 1 1 1	Host http://192.168.1.4 http://192.168.1.4 http://192.168.1.4 http://192.168.1.4 http://192.168.1.4 http://192.168.1.4 http://192.168.1.4 http://192.168.1.4 http://192.168.1.4	Met URL GET /formulaire: GET /forum3 GET /loorum3 GET /loots GET /formular GET /fav GET /fav GET /fav GET /finder GET /filestore		Edited Status c 404 404 404 404 404 404 404 4	Len         MIME           502         HTML           497         HTML           497         HTML           501         HTML           496         HTML           499         HTML           494         HTML           495         HTML           496         HTML           497         HTML           496         HTML           497         HTML           497         HTML           497         HTML           497         HTML           500         HTML	Exten Title 404 Not I 404 Not I	Notes           Found         -           Found         -	TLS IP 192.168.1.4 192.168.1.4 192.168.1.4 192.168.1.4 192.168.1.4 192.168.1.4 192.168.1.4 192.168.1.4 192.168.1.4 192.168.1.4 192.168.1.4	Cookies Time 05/36/4 05/36/4 05/36/4 05/36/4 05/36/4 05/36/4 05/36/4 05/36/4 05/36/4	Listene 	
Req	uest			Response				Inspector	■■ Ξ ÷ ©	× ÷	
Pret	tty Raw Hex	- UTTD/1 1	🗞 🚍 In	≡ Pretty R	aw Hex Re	ender Found	🗐 \n	≡ Request attribu		) Inspe	
2 A 3 L	Accept: */* Jser-Agent: fero	oxbuster/2.10	. 4	2 Date: 3 Serve	Sun, 11 Aug r: Apache/2	g 2024 09:36:4 .4.25 (Debian)	17 GMT	Request header	rs 5	× ctor	
4 0	Content-Type:	w-form-urlon	coded	4 Conter	nt-Length: :	286				B	
5 F 6 C 7	Host: 192.168.1 Connection: keep	.4 p-alive		6 Conner 7 Conter	nt-Type: te	-Alive xt/html; chars	set=iso-8859-1			] Notes	

#### 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 ferc	<b>ækali</b> xbuste	)-[~] r -u http:/	/192.168.1.4	cookies	PHPSES	SID=t54ij1	5l5d51i2	tc7j1k?	1tu4p4	burp -c	1 <b></b>		
404	GET	91	32w	-c Auto	o-filter:	ing found	<mark>404</mark> -like	e respo	nse and	created	new fil	lter;	to
403	GET	111	32w	-c Auto	o-filter:	ing found	404-like	e respo	nse and	created	new fil	lter:	to
302	GET	01	0w	0c httr	.://192. <sup>*</sup>	168.1.4/=	⇒ login.	nhn				,	
301	GET	91	2814	309c httr	1/192	168 1 4/do	$rs \rightarrow ht$	$tn \cdot 1/1$	92 168	1 //docs/			
201	CET	01	200	211c h++r	1/102	160.1.4/00	$c_3 \rightarrow nc$	b++p•// 1	$1/102 \cdot 100$	1.4/0003/	5:01		
201	GET	91	20W		(1402)		1112 = 2	nccp:/	/192.10	0.1.4/00	li 18/		
200	GEI	11	100	105C nttp	)://192	168.1.4/00	cs/pat.n	ינשנ					
200	GET	Ø L	Øw	0c http	<b>b://192.</b> 2	168.1.4/co	nfig/con	ntig.in	c.php				
200	GET	1.71	787111 *	IQGOC h++r		169 1 //co	nfig/con	ifia in	c nhn h	ak .			
Dura Daniant				burp suite comm	unity Euron v2024.5	.5 - Temporary Project							
Burp Project	Trunch	Repeater view He	elp Distantia Callabas								ŝ		
Dashboard	Target	Proxy Intruder	Repeater Collabor	ator Sequenci	er Decoder	Comparer I	Logger Orga	anizer E	xtensions	Learn	ŵ	Settings	
Intercept	HTTP histor	y WebSockets his	story   😲 Proxy sett	ings									te
🖓 Filter sett	ings: Hiding	CSS, image and gene										0 i	
#∽ Host					Len MIME .								
2 http://192	2.168.1.4	GET /ron		404	494 HTML	404 No	ot Found		192.168.	1.4	05:42:1	8080	
2 http://192	2.168.1.4				494 HTML	404 No	ot Found		192.168.	1.4	05:42:1		
2 http://192	2.168.1.4	GET /searchedit		404	501 HTML	404 No	ot Found		192.168.	1.4	05:42:1	8080	
2 http://192	2.168.1.4	GET /rechercher		404	501 HTML	404 No	ot Found		192.168.	1.4	05:42:1	8080	
2 http://192	2.168.1.4	GET /scripts2		404	499 HTML	404 No	ot Found		192.168.	1.4	05:42:1	8080	
2 http://192	2.168.1.4	GET /reserv		404	497 HTML	404 No	ot Found		192.168.	1.4	05:42:1		
2 http://192	2.168.1.4	GET /riders		404	497 HTML	404 No	ot Found		192.168.	1.4	05:42:1	8080	
2 http://192	2.168.1.4	GET /seasonal		404	499 HTML	404 No	ot Found		192.168.	1.4	05:42:1	8080	
2 http://19.	2.168.1.4	GET /searchprof	ıle	404	504 HTML	404 No	ot Found		192.168.	1.4	05:42:1	0808	
2 http://19.	2.108.1.4	GET /rsscacne		404	499 HIML	404 No 404 No	ot Found		192.168.	1.4 1 4	05:42:1	8080	
2 11(10.1/19.	2.106.1.4	GET /schuluhu		404	499 HTML	404 110			192.106.	1.4	03.47.1		
Request				Response					Inspector	•	≅ ÷ ©	× ⇔	
Pretty Ray			🗞 🚍 In 🗉	Pretty Ra	aw Hex R	ender		<b>≕</b> \n ≡	Request at	tributes		~ Ist	
1 GET /rs 2 Accept:	scache + */*	ITTP/1.1		1 HTTP/1 2 Date:	.1 404 Not Sun, 11 Au	Found g 2024 09:42	:11 GMT					> >	
3 User-Ac 4 Cookie:	ent: fer PHPSESS	roxbuster/2.10 SID=t54ij1515d	.4 51i2tc7j1k1t <u>u4p4</u>	3 Server 4 Con <u>ten</u>	: Apache/2 t-Lengt <u>h</u> :	.4.25 (Debia 283	n)		Request he				
5 Host: 1	92.168.1	1.4 		5 Keep-A	live: time	out=5, max=6	2		Response	neaders	6	~	

# 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

<pre>(root@kali)-[~]   feroxbuster -u http://1</pre>	92.168.1.4 -f 🚤
) ) /_``     ) /_`` by Ben "epi" Risher @	/
🎯 Target Url	http://192.168.1.4
🚀 Threads	50
📖 Wordlist	/usr/share/seclists/Discovery/Web-Content/raft-medium-director
👌 Status Codes	All Status <mark>Codes</mark> !
🕷 Timeout (secs)	7
🚗 User-Agent	feroxbuster/2.10.4
💉 Config File	/etc/feroxbuster/ferox-config.toml
Extract Links	true
HTTP methods	LGETJ
🔨 Add Slash	true
Recursion Depth	
🚨 Caught ctrl+c 🚨 saving :	scan state to ferox-http_192_168_1_4-1/23369419.state
[>	9281/10680031 6/m found:12 errors:0
[###>] - 4S	$4421/30000  1044/S  \text{http://192.168.1.4/} \Rightarrow \text{Wildcard dir!}$
$\begin{bmatrix} & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & $	$30000/30000 = 00015/S \text{ Http://192.100.1.4/u0037 } \Rightarrow \text{ Directory}$
$\begin{bmatrix} ++++++++++++++++++++++++++++++++++++$	$2974/20000 = 29297/5 \operatorname{Http://192.100.1.4/config} \implies \operatorname{Wildearc}$
$\begin{bmatrix} +++ \\ ++$	30000/30000 = 10000000/c  http://192.100.1.4/10013/  With the second secon
$\begin{bmatrix} + + + + + + + + + + + + + + + + + + +$	$30000/30000 = 1000000/3  http://192.108.1.4/external/ \rightarrow 0.1$
[ <del>************************************</del>	50000/50000 500000/5 http://192.108.1.4/externat/recapt

# 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

<b>.</b> ,	( <b>root®kali</b> )-[ <b>~</b> ] feroxbuster -u http://19	92.168.1.4burp 🚤
   by	)  )   / _`     _\   _\   / _` Ben "epi" Risher ☺	/
8 8 8 8 8 9 8 9 1 1 1 1 1 1 1 1 1 1 1 1 1	Target Url Threads Wordlist Status Codes Timeout (secs) User-Agent Config File Proxy Extract Links HTTP methods Insecure Recursion Depth	<pre>http://192.168.1.4 50 /usr/share/seclists/Discovery/Web-Content/raft-med All Status Codes! 7 feroxbuster/2.10.4 /etc/feroxbuster/ferox-config.toml http://127.0.0.1:8080 true [GET] true 4</pre>
pss	Press [ENTER] to use th	he Scan Management Menu™ 
[>- [>-	] - 269 ] - 269	s 62/30000 4h found:0 errors:60 s 63/30000 2/s http://192.168.1.4/
Burn Da:	o Project Intruder Repeater View Help shboard Target <u>Proxy</u> Intruder R <mark>ercept</mark> HTTP history WebSockets histo Request to http://192.168.1.4:80 Forward Drop <b>Intercept</b> i	Burp Suite Community Edition v2024.5.5 - Temporary Project Repeater Collaborator Sequencer Decoder Comparer Logger Organizer I ry  Ø Proxy settings s on Action Open browser
Pre	etty Raw Hex	کر <mark>کا</mark> ک
1 2 3 4 5 6 7	GET /admin7870e7a87e7d413bb01e168a 71a68 HTTP/1.1 Accept: */* User-Agent: feroxbuster/2.10.4 Host: 192.168.1.4 Connection: keep-alive	b23008d76f1cc5f3b45f4c908f50b87cde79296041e17e203f9f45d38a94eb4c

# 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

http://	ot© kali) t target. /192.168. //google. /192.168.	-[~] txt 1.4 com 1.5		
	ot®kali) t target.	-[ <b>~</b> ] <b>txt </b> ferox	busters	tdin -q 🚤
Could ⇒ e	not conne rror send	ct to http ing reques	://192.168 t for url	3.1.5, skipping (http://192.168.1.5/)
404	GEI	91	32W	-c Auto-filtering found 404-like re
403	GEI	111	32W	-c Auto-filtering found 404-like re
302	GET	01	0W 2.8w	$0C \operatorname{nup:}//192.168.1.4/ \Rightarrow \operatorname{login.pnp}_{200c}$
201	GET	91	20W	$3090 \text{ mtp:}//192.108.1.4/0000 \Rightarrow \text{mtp:}$
200		9L 11	20W 10w	$\frac{105c}{105c} + \frac{1}{100} + \frac{1}{100} + \frac{100}{100} + $
200	GET	471	10W 282W	1864c http://192.168.1.4/docs/pdf.ntmt
200	GET	47t 01	202W Øw	0c http://192.168.1 4/config/config
301	GET	91	28w	$313c \text{ http://192.168.1.4/external} \implies h$
200	GET	01	20W Øw	0c http://192.168.1.4/external/reca
301	GFT	91	28w	324c http://192.168.1.4/external/phpi
301	GET	61	14w	225c https://google.com/labs/ $\Rightarrow$ http
301	GET	61	14w	231c https://google.com/nonprofits/ =
301	GET	61	14w	235c https://google.com/commercesearc
301	GET	61	14w	226c https://google.com/forms/ $\Rightarrow$ htt
301	GET	61	14w	268c https://google.com/about/careers
301	GET	61	14w	257c https://google.com/about/careers
301	GET	61	14w	227c https://google.com/scholar ⇒ ht
301	GET	61	14w	258c https://google.com/about/careers
301	GET	61	14w	233c https://google.com/trends/topics
301	GET	61	14w	260c https://google.com/about/careers
301	GET	61	14w	235c https://google.com/hotelfinder/r
301	GET	61	14w	240c https://google.com/landing/cmsne
301	GET	61	14w	249c https://google.com/help/maps/ind
301	GET	61	14w	228c https://google.com/books/ ⇒ htt

## **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	<mark>⊕kali</mark> xbustei	)-[~] r -u http://	192.168.	1.4 -a
	6FT	0]		
404	GEI	9l 111	32W	-c Auto-filtering found 404-like response
405 302	GET	01 01	S∠W Øw	-c Auto-Fittering found 404-tike response
302	GET	91	28w	$309c \text{ http://192.108.1.4/} \rightarrow \text{togin.php}$
301	GET	91	28w	311c http://192.100.1.4/config => http://192.1
200	GET	11	10w	105c http://192.168.1.4/docs/pdf.html
200	GET	471	282w	1864c http://192.168.1.4/config/config.inc.ph
200	GET	471	282w	1859c http://192.168.1.4/config/config.inc.ph
200	GET	01	Øw	<pre>0c http://192.168.1.4/config/config.inc.ph</pre>
301	GET	91	28w	313c http://192.168.1.4/external $\Rightarrow$ http://1
301	GET	91	28w	324c http://192.168.1.4/external/phpids/0.6
200	GET	01	0w	0c http://192.168.1.4/external/recaptcha/r
404	GET	91	33w	287c http://192.168.1.4/Reports%20List
404	GET	91 01	33w	289c http://192.168.1.4/external%20files
404	GEI	9L 01	33W	288c http://192.168.1.4/Style%20Library
404	GEI	9L	33W 2400	285c http://192.168.1.4/modern%20mom
404 Sconning	0E1	9L //102 160 1	34W	290C nttp://192.168.1.4/neut%20g1ga%20pnoto
	t otal	.//192.100.1	4/	$r_{1}$
Scanning	• http:	• //192.168.1	. 4/	ate to refox-http_192_100_1_4-1725570170.state .
Scanning	: http:	://192.168.1		σ/
Scanning	: http:	://192.168.1	.4/exter	rnal/
Scanning	: http:	://192.168.1	.4/exter	rnal/recaptcha/
Scanning	: http:	://192.168.1		rnal/phpids/
<u> </u>				
(root fero	<mark>®kali</mark> xbustei	)-[ <b>~</b> ] rresume-f	rom <b>fero</b>	ox-http_192_168_1_4-1723370176.state -q 🛶
302	GET	01	Øw	0c http://192.168.1.4/ $\Rightarrow$ login.php
301	GET	91	28w	309c http://192.168.1.4/docs ⇒ http://192.1
301	GET	91	28w	311c http://192.168.1.4/config => http://192
200	GET	11	10w	105c http://192.168.1.4/docs/pdf.html
200	GEI	4/L	282w	1864c http://192.168.1.4/config/config.inc.ph
200	GEI	4/1	282W	1859C nttp://192.168.1.4/config/config.inc.pn
200	GET	0L 01	0W 2.8w	$\frac{1}{2} = \frac{1}{2} + \frac{1}$
301 301	GET	9L 01	20W 28w	$324c$ http://192.108.1.4/external $\rightarrow$ http://1
200	GET	91 01	20w	0c http://192.168.1.4/external/recantcha/r
404	GFT	91	33w	287c http://192.168.1.4/Reports%20List
404	GET	91	33w	289c http://192.168.1.4/external%20files
404	GET	91	33w	288c http://192.168.1.4/Style%20Library
404	GET	91	33w	285c http://192.168.1.4/modern%20mom
404	GET	91	34w	290c http://192.168.1.4/neuf%20giga%20photo
404	GET	91	32w	-c Auto-filtering found 404-like response
403	GET	11l	32w	-c Auto-filtering found 404-like response
200	GET	29221	17217w	730335c http://192.168.1.4/docs/DVWA_v1.3.pdf
404	GET	91	33w	285c http://192.168.1.4/Contact%20Us
404	GET	91	33w	286c http://192.168.1.4/Donate%20Cash
404	GET	91	33w	284c http://192.168.1.4/Home%20Page
404	GET	91	33w	289c http://192.168.1.4/Planned%20Giving
404	GET	91	33w	283c http://192.168.1.4/Site%20Map
Scanning	: http:	.7/192.168.1	.4/confi	
Sconning	t CTrl+	FC 🚨 Saving	scan st	Late to ferox-http_192_168_1_4-1/233/019/.state .
Scanning	• http:	•//192.168.1 •//102 160 1		
Scanning	• http:	• //192.108.1 • //192 <u>_168_1</u>	4/exter	rnal/recant cha/
Scanning	: http:	://192.168.1	.4/exter	nal/nhnids/
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.

fero	eroxbuster -u http://192.168.1.4 -r								
(	root@kali)	-[~]							
L_#`									
			-, <i>_</i>	\_/     <sup>−</sup>					
			_, \_/	/ \    _	_/				
by E	3en "epi" Ri	sher 🤓		ver:	2.10.4				
6	Target Url		http:/	//192.168	3.1.4				
1	Threads		50						
	Wordlist		/usr/s	hare/sec	lists/Discovery/Web-Content/raft-medium-direc				
<b></b>	Status Cod	es occ)	ALL St	atus Coc	16S !				
~	User-Agent	ets)	feroxb	uster/2	10.4				
A	Config Fil	e	/etc/f	eroxbust	cer/ferox-config.toml				
ø	Extract Li	nks	true		-				
pss .	HTTP metho	ds	[GET]						
	Follow Red	lrects Donth	true						
<b>p</b> 88	Press [ENT	ER] to use	e the <mark>Scan</mark>	Manageme	ent Menu™				
403	GET	11l	32w	- c	Auto-filtering found 404-like response and cr				
404	GET	91	32w	- C	Auto-filtering found 404-like response and cr				
200	GET	591	101w	842c	http://192.168.1.4/dvwa/css/login.css				
200	GET	1l 101	10W 05w	105C 8064c	http://192.168.1.4/docs/pdf.html				
200	GET	181 01	93W Øw	0004C 0C	http://192.168.1.4/config/config.inc.php				
200	GET	471	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	01	Øw	0c	http://192.168.1.4/external/recaptcha/recaptc				
200	GET	165l	1234w	7639c	<pre>http://192.168.1.4/external/phpids/0.6/LICENS</pre>				
200	GET	18l	24w	380c	http://192.168.1.4/external/phpids/0.6/build.				
404	GET	9L 01	33W 33W	287C 289c	http://192.108.1.4/Reports%20List				
404	GET	91	33w	289C	http://192.168.1.4/Style%20Library				
200	GET	251	36w	304c	http://192.168.1.4/dvwa/css/help.css				
200	GET	201	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	391	244w	16182c	http://192.168.1.4/dvwa/images/login_logo.png				
200	GET	771	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	391	99W	1030c	http://192.168.1.4/dvwa/js/dvwaPage.js				
404	GET	91	34w	285C	http://192.168.1.4/moderna20mom				

#### Timeout

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

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

[ <mark>#</mark> (	<b>root@kali</b> )-[ <b>~</b> ] feroxbuster -u http://19	92.168.1.4 -
   by B	)  )   / ``     ∖   ∖   en "epi" Risher ☺	/
© #	Target Url Threads	http://192.168.1.4 50
244 244	Wordlist Status Codes Timeout (secs)	/usr/share/seclists/Discovery All Status Codes!
* ***	User-Agent Config File	feroxbuster/2.10.4
) 	Extract Links HTTP methods	true [GET]
t)	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



#### **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



in 😱

www.ignitetechnologies.in