

“DIRB”

---S.JOE MATHEW
(192IT159)

Dirb is a CLI directory buster which checks all the possible directories in the website from the wordlist given by dirb. When we type **dirb** all options are shown.

```
root@kali:~# dirb

-----
DIRB v2.22
By The Dark Raver
-----

dirb <url_base> [<wordlist_file(s)>] [<options>]

===== NOTES =====
<url_base> : Base URL to scan. (Use -resume for session resuming)
<wordlist_file(s)> : List of wordfiles. (wordfile1,wordfile2,wordfile3...)

===== HOTKEYS =====
'n' -> Go to next directory.
'q' -> Stop scan. (Saving state for resume)
'r' -> Remaining scan stats.

===== OPTIONS =====
-a <agent_string> : Specify your custom USER_AGENT.
-b : Use path as is.
-c <cookie_string> : Set a cookie for the HTTP request.
-E <certificate> : path to the client certificate.
-f : Fine tuning of NOT_FOUND (404) detection.
-H <header_string> : Add a custom header to the HTTP request.
-i : Use case-insensitive search.
-l : Print "Location" header when found.
-N <nf_code>: Ignore responses with this HTTP code.
-o <output_file> : Save output to disk.
-p <proxy[:port]> : Use this proxy. (Default port is 1080)
-P <proxy_username:proxy_password> : Proxy Authentication.
-r : Don't search recursively.
-R : Interactive recursion. (Asks for each directory)
-S : Silent Mode. Don't show tested words. (For dumb terminals)
-t : Don't force an ending '/' on URLs.
-u <username:password> : HTTP Authentication.
-v : Show also NOT_FOUND pages.
-w : Don't stop on WARNING messages.
-X <extensions> / -x <exts_file> : Append each word with this extensions.
```

USAGE:

1.Common usage is **dirb http://testphp.vulnweb.com** list all possible directories in the website from the default wordlist **common.txt**

```
root@kali: /usr/share/wordlists/dirb# dirb http://testphp.vulnweb.com

-----
DIRB v2.22
By The Dark Raver
-----

START TIME: Sun Jun 28 19:19:12 2020
URL_BASE: http://testphp.vulnweb.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://testphp.vulnweb.com/ ----
=> DIRECTORY: http://testphp.vulnweb.com/admin/
+ http://testphp.vulnweb.com/cgi-bin/ (CODE:403|SIZE:263)
+ http://testphp.vulnweb.com/cgi-bin/ (CODE:403|SIZE:263)
+ http://testphp.vulnweb.com/crossdomain.xml (CODE:200|SIZE:224)
=> DIRECTORY: http://testphp.vulnweb.com/CVS/
+ http://testphp.vulnweb.com/CVS/Entries (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/CVS/Repository (CODE:200|SIZE:8)
+ http://testphp.vulnweb.com/CVS/Root (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/favicon.ico (CODE:200|SIZE:894)
=> DIRECTORY: http://testphp.vulnweb.com/images/
+ http://testphp.vulnweb.com/index.php (CODE:200|SIZE:4958)
=> DIRECTORY: http://testphp.vulnweb.com/pictures/
=> DIRECTORY: http://testphp.vulnweb.com/secured/
```

2. There are also many wordlist in **usr/share/dirb/wordlists**

```
root@kali: /usr/share/dirb/wordlists# ls -l
total 260
-rw-r--r-- 1 root root 184073 Qun 25 2012 big.txt
-rw-r--r-- 1 root root 1292 Qun 27 2012 catala.txt
-rw-r--r-- 1 root root 35849 Xim 17 2014 common.txt
-rw-r--r-- 1 root root 1492 Cax 23 2012 euskera.txt
-rw-r--r-- 1 root root 142 Kax 29 2005 extensions_common.txt
-rw-r--r-- 1 root root 75 Cig 16 2012 indexes.txt
-rw-r--r-- 1 root root 244 Kax 29 2005 mutations_common.txt
drwxr-xr-x 2 root root 4096 Agd 18 13:50 others
-rw-r--r-- 1 root root 6561 Cig 5 2014 small.txt
-rw-r--r-- 1 root root 3731 Xim 13 2014 spanish.txt
drwxr-xr-x 2 root root 4096 Agd 18 13:50 stress
drwxr-xr-x 2 root root 4096 Agd 18 13:50 vulns
```

We can use **small.txt** so command is **dirb http://testphp.vulnweb.com/ /usr/share/dirb/wordlists/small.txt**

```

root@kali:~/usr/share/dirb/wordlists# dirb http://testphp.vulnweb.com/ /usr/share/dirb/wordlists/small.txt
-----
DIRB v2.22
By The Dark Raver
-----
START_TIME: Sun Jun 28 19:27:09 2020
URL_BASE: http://testphp.vulnweb.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/small.txt

----- http://testphp.vulnweb.com/ ----
=> DIRECTORY: http://testphp.vulnweb.com/admin/
GENERATED WORDS: 959
----- Scanning URL: http://testphp.vulnweb.com/ ----
=> DIRECTORY: http://testphp.vulnweb.com/ CVS/ (CODE:200|SIZE:224)
=> DIRECTORY: http://testphp.vulnweb.com/admin/
+ http://testphp.vulnweb.com/cgi-bin/ (CODE:403|SIZE:263)
+ http://testphp.vulnweb.com/cgi-bin/ (CODE:403|SIZE:263)
=> DIRECTORY: http://testphp.vulnweb.com/images/ (CODE:200|SIZE:17)
=> DIRECTORY: http://testphp.vulnweb.com/secured/ (CODE:200|SIZE:894)

----- Entering directory: http://testphp.vulnweb.com/ CVS/ -----
----- Entering directory: http://testphp.vulnweb.com/admin/ -----
----- Entering directory: http://testphp.vulnweb.com/images/ -----
----- Entering directory: http://testphp.vulnweb.com/secured/ -----

----- http://testphp.vulnweb.com/admin/graphics
END_TIME: Sun Jun 28 19:46:04 2020
DOWNLOADED: 4795 - FOUND: 2

```

3. If we want a directory with specific extension i am using .php extension and i want to save the output to a file .

Command: **dirb http://testphp.vulnweb.com / -X .php -o out.txt**

```

root@kali:~/dirb# dirb http://testphp.vulnweb.com/ -X .php -o out.txt
-----
DIRB v2.22
By The Dark Raver
-----
OUTPUT_FILE: out.txt
START_TIME: Sun Jun 28 19:29:19 2020
URL_BASE: http://testphp.vulnweb.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]

-----
GENERATED WORDS: 4612

----- Scanning URL: http://testphp.vulnweb.com/ ----
+ http://testphp.vulnweb.com/404.php (CODE:200|SIZE:5265)
+ http://testphp.vulnweb.com/artists.php (CODE:200|SIZE:5328)
+ http://testphp.vulnweb.com/cart.php (CODE:200|SIZE:4903)
+ http://testphp.vulnweb.com/categories.php (CODE:200|SIZE:6115)
+ http://testphp.vulnweb.com/comment.php (CODE:302|SIZE:1246)
+ http://testphp.vulnweb.com/disclaimer.php (CODE:200|SIZE:5524)
+ http://testphp.vulnweb.com/guestbook.php (CODE:200|SIZE:5390)
+ http://testphp.vulnweb.com/index.php (CODE:200|SIZE:4958)
+ http://testphp.vulnweb.com/login.php (CODE:200|SIZE:5523)
+ http://testphp.vulnweb.com/logout.php (CODE:200|SIZE:4830)
+ http://testphp.vulnweb.com/product.php (CODE:200|SIZE:5056)
+ http://testphp.vulnweb.com/redirect.php (CODE:302|SIZE:0)
+ http://testphp.vulnweb.com/search.php (CODE:200|SIZE:4732)
+ http://testphp.vulnweb.com/signup.php (CODE:200|SIZE:6033)
+ http://testphp.vulnweb.com/userinfo.php (CODE:302|SIZE:14)

-----
END_TIME: Sun Jun 28 19:47:58 2020
DOWNLOADED: 4612 - FOUND: 15

root@kali:~/dirb# ls
out.txt

```


4. In this we don't want directories with status code -N 302 (NOT FOUND) -w is verbose mode -r is not traverse recursive the directories

COMMAND:> **dirb http://testphp.vulnweb.com/ -N 302 -w -r**

```
root@kali:~# dirb http://testphp.vulnweb.com/ -N 302 -w -r

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Sun Jun 28 19:31:57 2020
URL_BASE: http://testphp.vulnweb.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Ignoring NOT_FOUND code → 302
OPTION: Not Recursive
OPTION: Not Stopping on warning messages

-----
GENERATED WORDS: 4612

---- Scanning URL: http://testphp.vulnweb.com/ ----
=> DIRECTORY: http://testphp.vulnweb.com/admin/
+ http://testphp.vulnweb.com/cgi-bin (CODE:403|SIZE:263)
+ http://testphp.vulnweb.com/cgi-bin/ (CODE:403|SIZE:263)
+ http://testphp.vulnweb.com/crossdomain.xml (CODE:200|SIZE:224)
=> DIRECTORY: http://testphp.vulnweb.com/CVS/
+ http://testphp.vulnweb.com/CVS/Entries (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/CVS/Repository (CODE:200|SIZE:8)
+ http://testphp.vulnweb.com/CVS/Root (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/favicon.ico (CODE:200|SIZE:894)
=> DIRECTORY: http://testphp.vulnweb.com/images/
+ http://testphp.vulnweb.com/index.php (CODE:200|SIZE:4958)
=> DIRECTORY: http://testphp.vulnweb.com/pictures/
=> DIRECTORY: http://testphp.vulnweb.com/secured/

-----
END_TIME: Sun Jun 28 19:50:28 2020
DOWNLOADED: 4612 - FOUND: 8
```

5. Now we login and list all directories after the login page .

COMMAND : **dirb http://testphp.vulnweb.com/login.php -u test:test**
(-u username: password)

```
root@kali:~# dirb http://testphp.vulnweb.com/login.php -u test:test

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Sun Jun 28 19:33:39 2020
URL_BASE: http://testphp.vulnweb.com/login.php/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
AUTHORIZATION: test:test
OPTION: Not Recursive
OPTION: Not Stopping on warning messages

-----
GENERATED WORDS: 4612

---- Scanning URL: http://testphp.vulnweb.com/login.php/ ----
+ http://testphp.vulnweb.com/login.php/admin.php (CODE:200|SIZE:5523)
+ http://testphp.vulnweb.com/login.php/index.php (CODE:200|SIZE:5523)
+ http://testphp.vulnweb.com/login.php/info.php (CODE:200|SIZE:5523)
+ http://testphp.vulnweb.com/login.php/phpinfo.php (CODE:200|SIZE:5523)
+ http://testphp.vulnweb.com/login.php/xmlrpc.php (CODE:200|SIZE:5523)
+ http://testphp.vulnweb.com/login.php/xmlrpc_server.php (CODE:200|SIZE:5523)

-----
END_TIME: Sun Jun 28 19:52:25 2020
DOWNLOADED: 4612 - FOUND: 6
```

--THANK YOU