logo

Gobuster Cheatsheet

Gobuster Cheatsheet

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

The help section can provide options for Gobuster.

> gobuster -h

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

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

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

Common Command line options

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

Command line options for dns mode

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

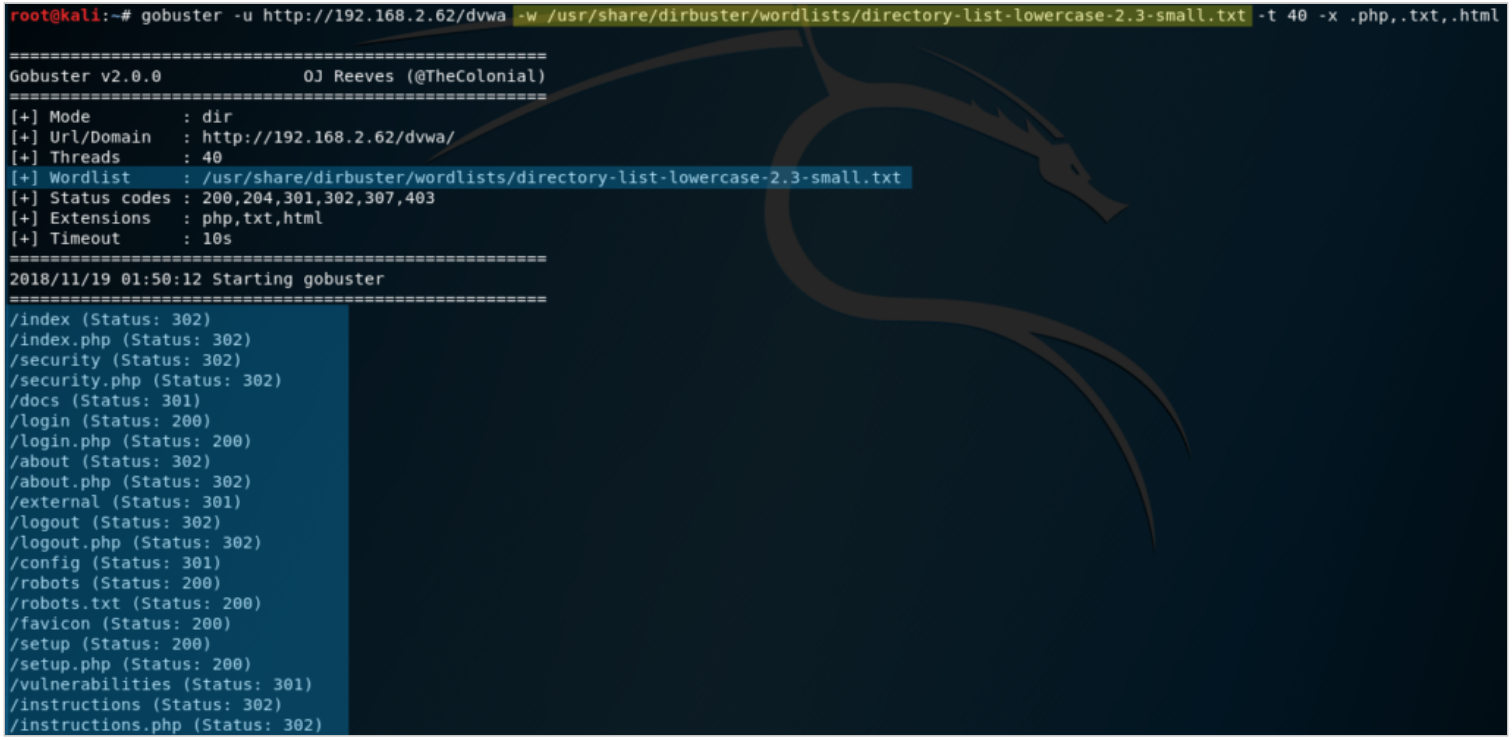
Command line options for dir mode

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

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

Wordlist Usage

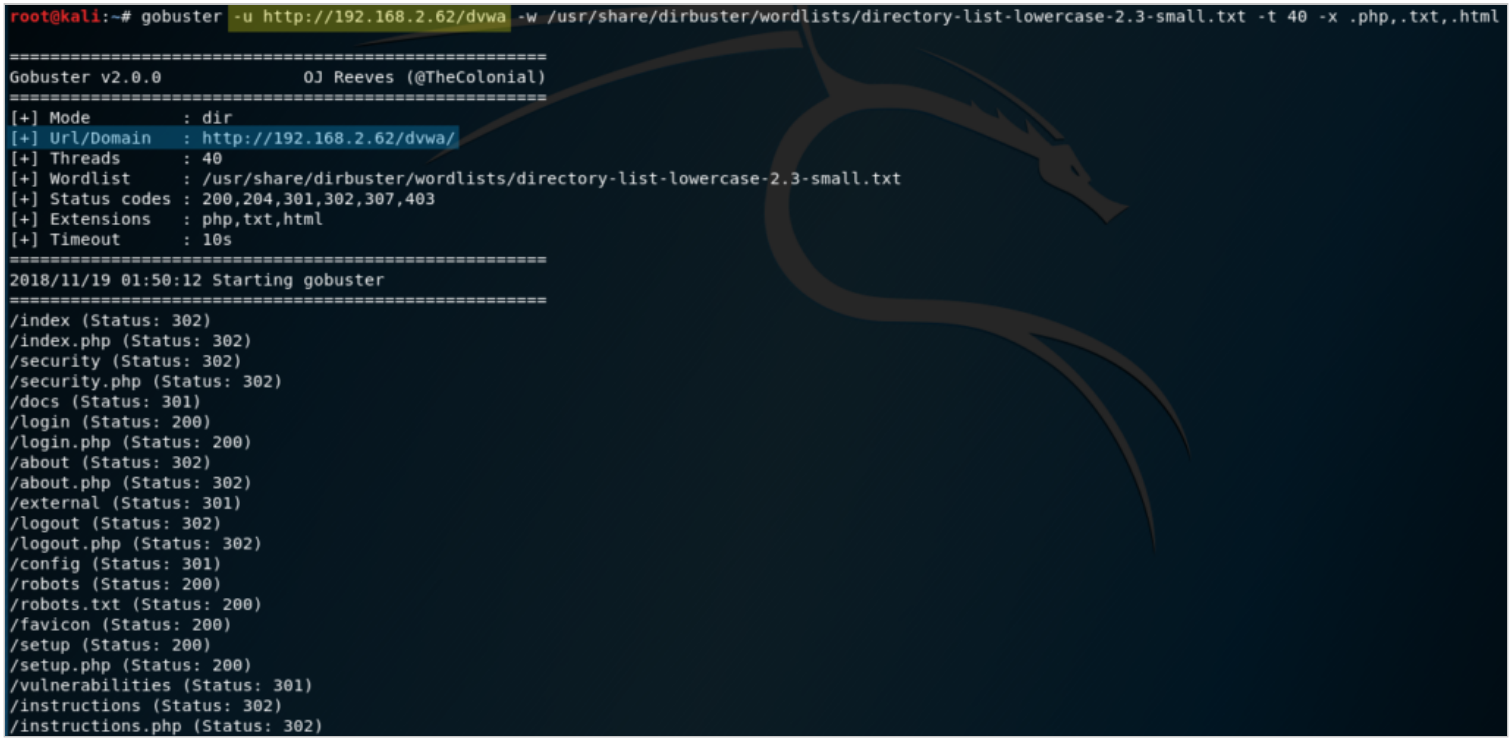
> “ gobuster -w <wordlist.txt>”



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

URL Usage

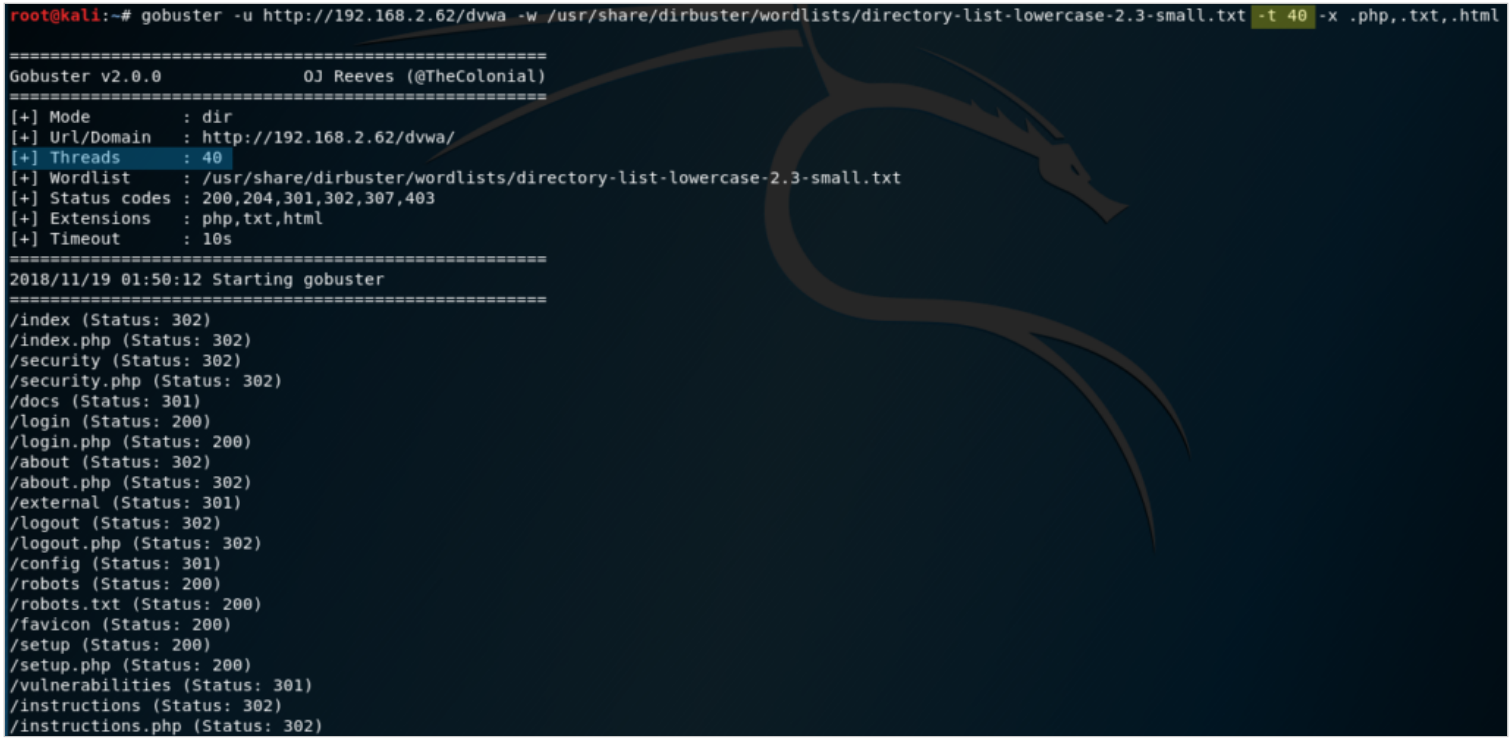
> gobuster -u <url>



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

Thread Usage

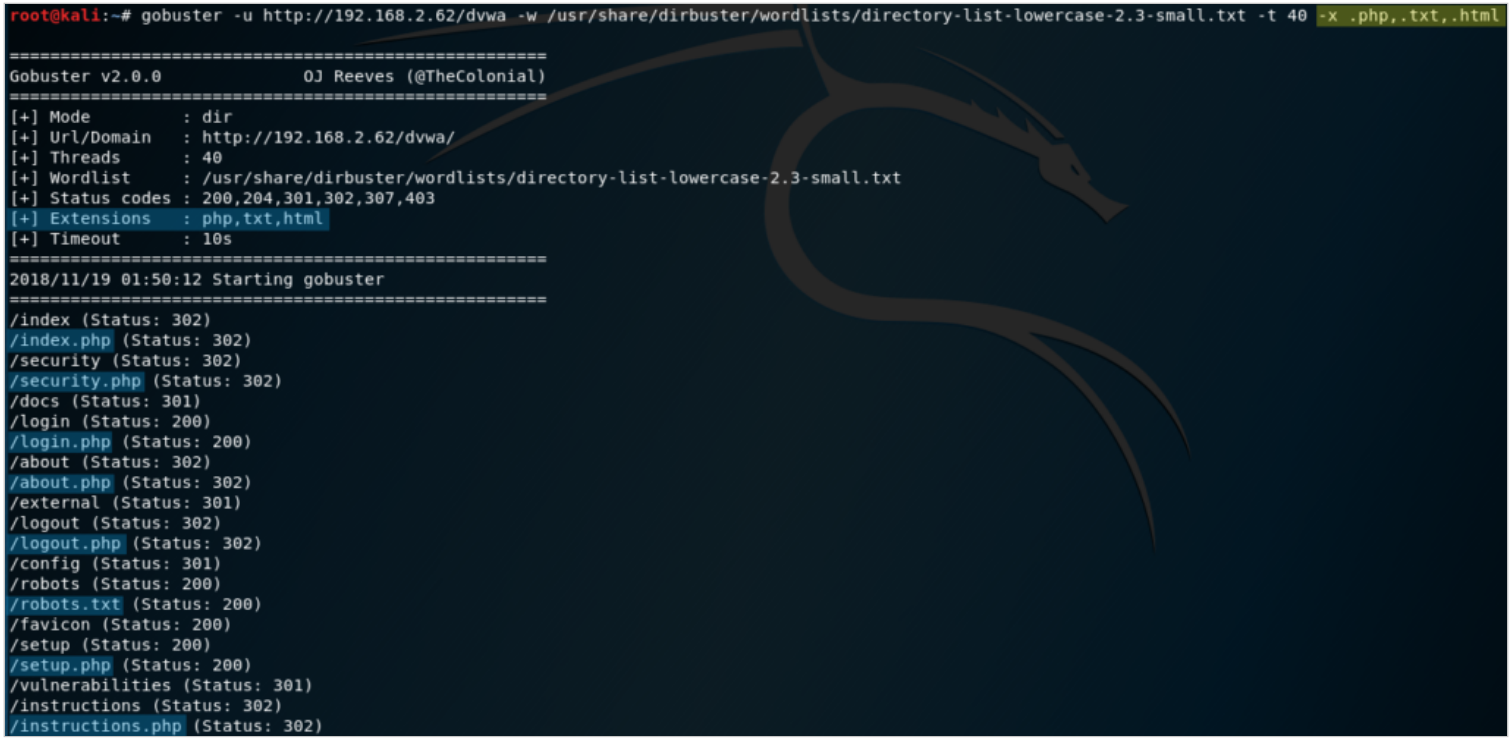
> gobuster -t <Num>



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

Extension Usage

> “ gobuster -x <ext>”



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

String Usage

> “ gobuster -s “<string>” ”

The string switch species the results that are being displayed.

Expanded Mode Usage

> “ gobuster -e”

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

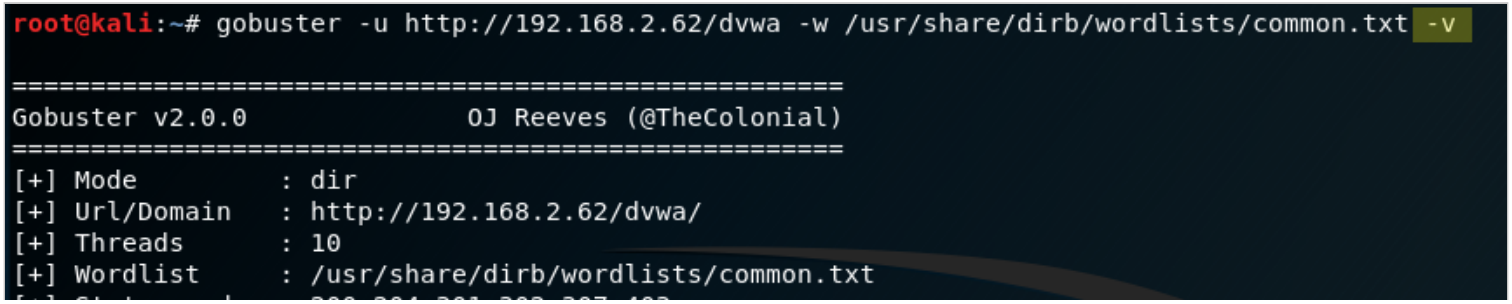
No Status Usage

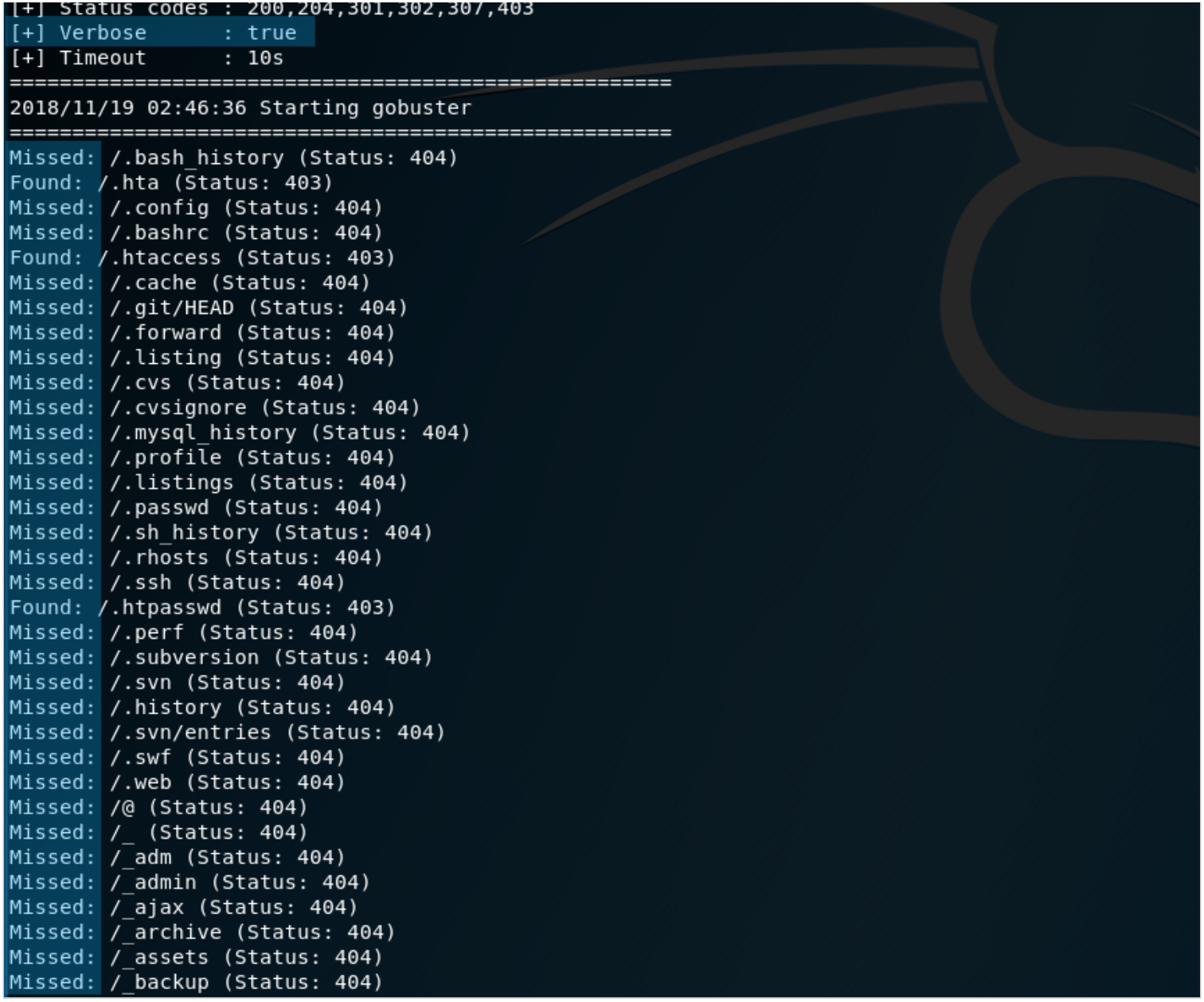
> gobuster -n

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

Verbose Mode

> gobuster -v

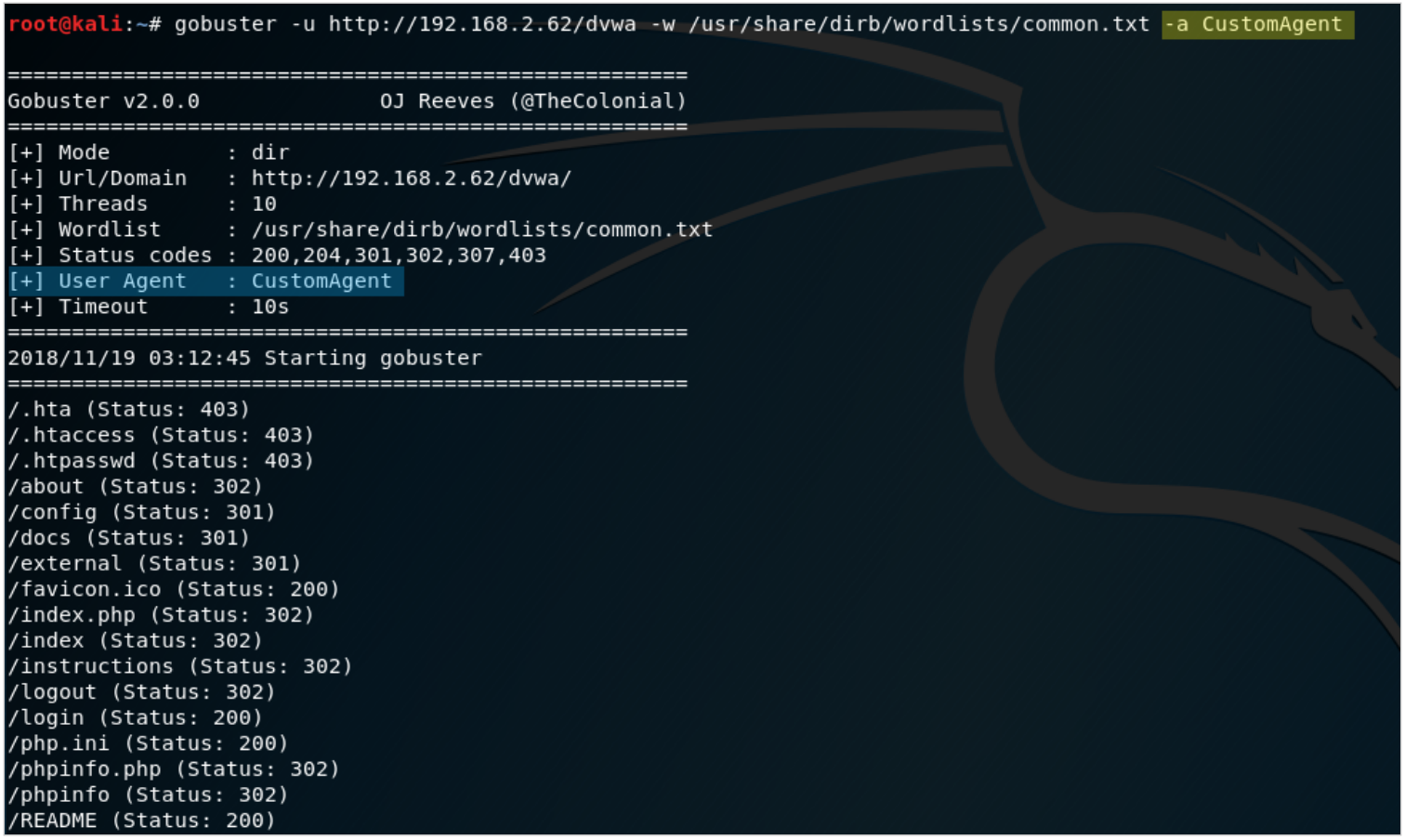




The verbose mode will increase the logging level of the search results.

User Agent

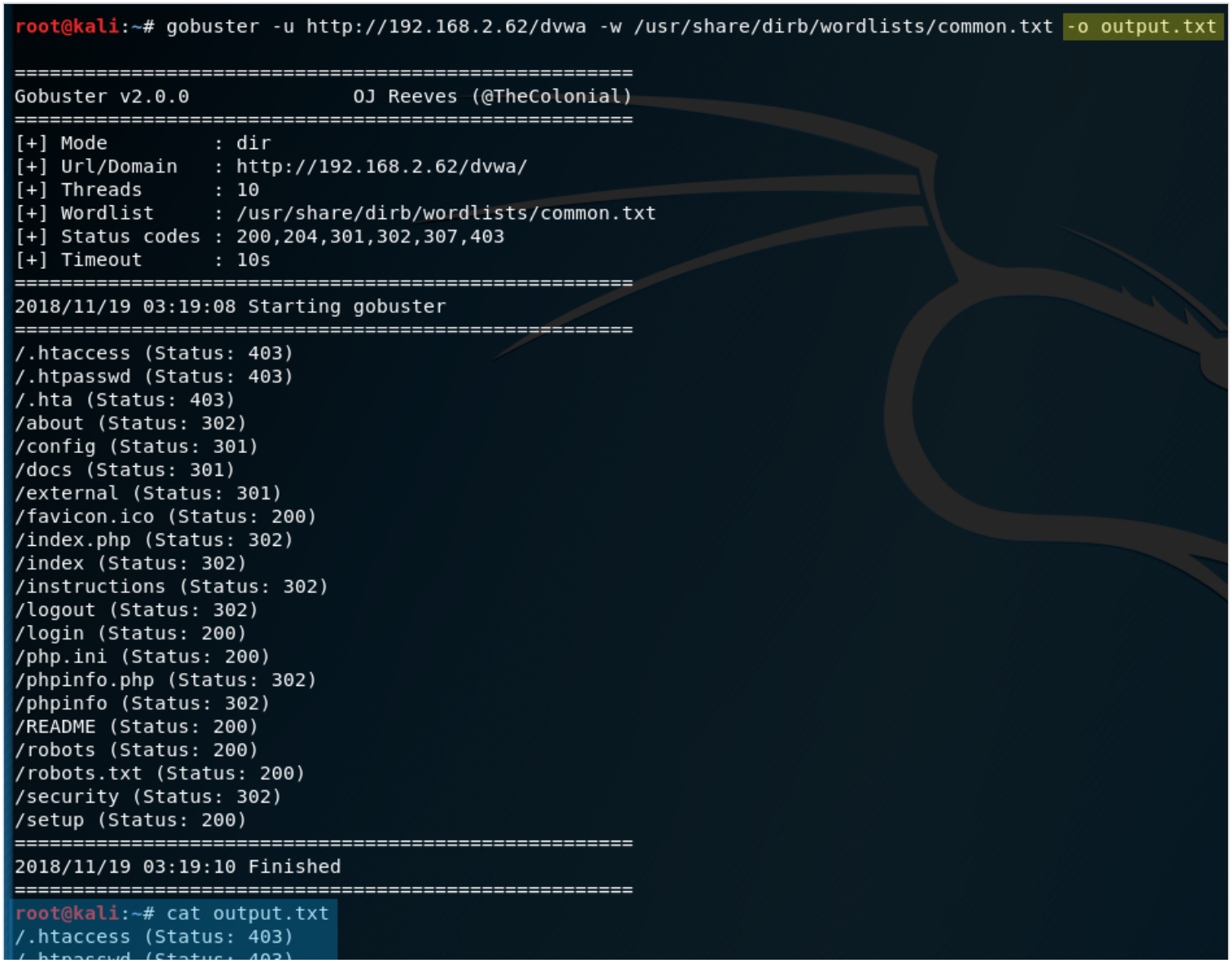
> gobuster -a <useragent>



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

Export Option

> gobuster -o <filename>



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

Previous post
Hack The Box: Brainf#@k

Next post
Hack The Box: Sense