



# Dirsearch

Website brute-forcing



## Table of Contents

Abstract.....	3
Introduction.....	4
<b>Target URL</b> .....	6
<b>Save Output in Different Formats</b> .....	7
<b>No Colour</b> .....	14
<b>Quite Mode</b> .....	14
<b>Normal scan vs Recursive scan</b> .....	15
<b>Post method</b> .....	18
<b>Delay request</b> .....	20
<b>Version scan</b> .....	21
Conclusion .....	21
References .....	21



## Abstract

Dirsearch is a simple command-line tool designed to brute force directories and files in websites. It is a Python-based command-line website directory scanner designed to brute force site structure including directories and files.

In this report, we will learn how we can use some of Dirsearch's core functions.

**Disclaimer: This report is provided for educational and informational purpose only (Penetration Testing). Penetration Testing refers to legal intrusion tests that aim to identify vulnerabilities and improve cybersecurity, rather than for malicious purposes.**



# Introduction

Dirsearch is a professional command-line method for the brute force of web server folders and files. It has now become the top Web content scanner with many years of success.

It provides users with the ability to explore complex web content as a feature-rich tool, with many wordlist vectors, high accuracy, impressive performance, advanced connection/request settings, modern brute-force techniques and nice results.

It is a strong competitor in the directory scanner arena, with features such as multi-threading, proxy support, request latency, user agent randomization, and support for multiple extensions.

## Setup

It is a Python-written method used to brute-force web directories and files that are secret. It can run on Windows, Linux, and macOS, and provides a simple but powerful interface for the command line.

We are installing this tool in our kali, using the git-clone command to install Dirsearch web content scanner tool.

```
git clone https://github.com/maurosoria/dirsearch.git
```

```
root@kali:~# git clone https://github.com/maurosoria/dirsearch.git
Cloning into 'dirsearch' ...
remote: Enumerating objects: 13, done.
remote: Counting objects: 100% (13/13), done.
remote: Compressing objects: 100% (13/13), done.
remote: Total 6978 (delta 3), reused 1 (delta 0), pack-reused 6965
Receiving objects: 100% (6978/6978), 19.54 MiB | 2.16 MiB/s, done.
Resolving deltas: 100% (4549/4549), done.
```

After installing this tool, we need to navigate through its directories and search for dirsearch.py. Now, all we need just run this python written tool with [-h] parameter through this we can see all its parameter with their functions.

```
./dirsearch.py -h
```



```
root@kali:~# ls
dirsearch
root@kali:~# cd dirsearch/
root@kali:~/dirsearch# ls
CHANGELOG.md  db  dirsearch.py  lib  README.md  requirements.txt
CONTRIBUTORS.md  default.conf  Dockerfile  logs  reports  thirdparty
root@kali:~/dirsearch# ./dirsearch.py -h
Usage: dirsearch.py [-u|--url] target [-e|--extensions] extensions [options]

Options:
  --version          show program's version number and exit
  -h, --help         show this help message and exit

Mandatory:
  -u URL, --url=URL   Target URL
  -l FILE, --url-list=FILE
                     URL list file
  --stdin            URL list from STDIN
  --cidr=CIDR        Target CIDR
  -e EXTENSIONS, --extensions=EXTENSIONS
                     Extension list separated by commas (Example: php,asp)
  -X EXTENSIONS, --exclude-extensions=EXTENSIONS
                     Exclude extension list separated by commas (Example:
                     asp,jsp)
  -f, --force-extensions
                     Add extensions to the end of every wordlist entry. By
                     default dirsearch only replaces the %EXT% keyword with
                     extensions

Dictionary Settings:
  -w WORDLIST, --wordlists=WORDLIST
                     Customize wordlists (separated by commas)
  --prefixes=PREFIXES
                     Add custom prefixes to all entries (separated by
                     commas)
  --suffixes=SUFFIXES
                     Add custom suffixes to all entries, ignore directories
                     (separated by commas)
  --only-selected    Only entries with selected extensions or no extension
                     + directories
  --remove-extensions
                     Remove extensions in all wordlist entries (Example:
                     admin.php → admin)
  -U, --uppercase    Uppercase wordlist
  -L, --lowercase    Lowercase wordlist
  -C, --capital      Capital wordlist
```

Let's get started



## Target URL

We can use our web content scanner on a specific targeted URL with the help of [-u] parameter. To get appropriate results we need to make sure that it is an authenticated URL follow this command to get the desired results.

```
./dirsearch.py -u http://testphp.vulnweb.com/
```

As we can see we got some web directories and web pages.

```
root@kali:~/dirsearch# ./dirsearch.py -u http://testphp.vulnweb.com/
dirsearch v0.4.1
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10831
Error Log: /root/dirsearch/logs/errors-21-01-08_22-33-11.log
Target: http://testphp.vulnweb.com/
Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-08_22-33-12.txt

[22:33:12] Starting:
[22:33:23] 301 - 169B - /.idea → http://testphp.vulnweb.com/.idea/
[22:33:23] 200 - 951B - /.idea/
[22:33:23] 200 - 6B - /.idea/.name
[22:33:23] 200 - 171B - /.idea/encodings.xml
[22:33:23] 200 - 266B - /.idea/misc.xml
[22:33:23] 200 - 275B - /.idea/modules.xml
[22:33:23] 200 - 173B - /.idea/vcs.xml
[22:33:23] 200 - 143B - /.idea/scopes/scope_settings.xml
[22:33:23] 200 - 12KB - /.idea/workspace.xml
[22:33:34] 200 - 5KB - /404.php
[22:33:36] 200 - 595B - /CVS/
[22:33:36] 200 - 1B - /CVS/Root
[22:33:36] 200 - 1B - /CVS/Entries
[22:33:36] 301 - 169B - /Connections → http://testphp.vulnweb.com/Connections/
[22:33:43] 200 - 400B - /_mmServerScripts/
[22:33:43] 200 - 93B - /_mmServerScripts/MMHTTPDB.php
[22:33:49] 301 - 169B - /admin → http://testphp.vulnweb.com/admin/
[22:33:51] 200 - 262B - /admin/
[22:33:51] 200 - 262B - /admin?/login
[22:34:23] 200 - 5KB - /cart.php
[22:34:23] 403 - 276B - /cgi-bin/
[22:34:23] 403 - 276B - /cgi-bin
[22:34:31] 200 - 224B - /crossdomain.xml
[22:34:41] 200 - 894B - /favicon.ico
[22:34:49] 301 - 169B - /images → http://testphp.vulnweb.com/images/
[22:34:49] 200 - 377B - /images/
[22:34:50] 200 - 5KB - /index.php
[22:34:50] 200 - 3KB - /index.bak
[22:34:50] 200 - 3KB - /index.zip
[22:34:57] 200 - 5KB - /login.php
[22:34:58] 200 - 5KB - /logout.php
[22:35:15] 301 - 169B - /pictures → http://testphp.vulnweb.com/pictures/
[22:35:23] 200 - 5KB - /search.php
[22:35:24] 301 - 169B - /secured → http://testphp.vulnweb.com/secured/
[22:35:28] 200 - 6KB - /signup.php
[22:35:40] 302 - 14B - /userinfo.php → login.php

Task Completed
```



## Save Output in Different Formats

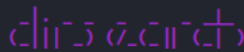
We can save our output which we get from the attack in different-different formats to learn further from them. This parameter helps us to get through those details of these formats. Let's explore them one by one.

### Save output in Simple format

We can save our result in the simple format with the help of `[-simple-report]` parameter. Through this feature, we can better analyse the results which we got from this attack. Follow this command to proceed further.

```
./dirsearch.py -u http://testphp.vulnweb.com/ --simple-report=report
```

```
root@kali:~/dirsearch# ./dirsearch.py -u http://testphp.vulnweb.com/ --simple-report=report



v0.4.1


Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10831
Error Log: /root/dirsearch/logs/errors-21-01-08_22-42-21.log
Target: http://testphp.vulnweb.com/
Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-08_22-42-21.txt

[22:42:21] Starting:
[22:42:35] 200 - 951B - /.idea/
[22:42:35] 200 - 6B - /.idea/.name
[22:42:35] 301 - 169B - /.idea → http://testphp.vulnweb.com/.idea/
[22:42:35] 200 - 275B - /.idea/modules.xml
[22:42:35] 200 - 266B - /.idea/misc.xml
[22:42:35] 200 - 171B - /.idea/encodings.xml
[22:42:35] 200 - 12KB - /.idea/workspace.xml
[22:42:36] 200 - 143B - /.idea/scopes/scope_settings.xml
[22:42:36] 200 - 173B - /.idea/vcs.xml
[22:42:51] 200 - 5KB - /404.php
[22:42:53] 200 - 595B - /CVS/
[22:42:54] 200 - 1B - /CVS/Entries
[22:42:54] 200 - 1B - /CVS/Root
[22:42:54] 301 - 169B - /Connections → http://testphp.vulnweb.com/Connections/
[22:43:06] 200 - 400B - /_mmServerScripts/
[22:43:06] 200 - 93B - /_mmServerScripts/MMHTTPDB.php
[22:43:11] 301 - 169B - /admin → http://testphp.vulnweb.com/admin/
[22:43:12] 200 - 262B - /admin/
[22:43:12] 200 - 262B - /admin/?/login
[22:43:41] 200 - 5KB - /cart.php
[22:43:41] 403 - 276B - /cgi-bin/
[22:43:41] 403 - 276B - /cgi-bin
[22:43:47] 200 - 224B - /crossdomain.xml
[22:43:59] 200 - 894B - /favicon.ico
[22:44:04] 301 - 169B - /images → http://testphp.vulnweb.com/images/
[22:44:04] 200 - 377B - /images/
[22:44:06] 200 - 5KB - /index.php
[22:44:06] 200 - 3KB - /index.bak
[22:44:06] 200 - 3KB - /index.zip
[22:44:14] 200 - 5KB - /login.php
[22:44:15] 200 - 5KB - /logout.php
[22:44:32] 301 - 169B - /pictures → http://testphp.vulnweb.com/pictures/
[22:44:40] 200 - 5KB - /search.php
[22:44:41] 301 - 169B - /secured → http://testphp.vulnweb.com/secured/
[22:44:44] 200 - 6KB - /signup.php
[22:44:56] 302 - 14B - /userinfo.php → login.php

Task Completed
```



After creating this report, we can cross verify its location in the system. Now use nano command to see this report.

```
root@kali:~/dirsearch# ls
CHANGELOG.md  db          dirsearch.py  lib  README.md  reports  thirdparty
CONTRIBUTORS.md  default.conf  Dockerfile    logs  report      requirements.txt
root@kali:~/dirsearch# nano report
```

As we can clearly see that our simple format result is successfully created. Now, we can analyse our results easily.

```
GNU nano 5.4 report
http://testphp.vulnweb.com:80/.idea/
http://testphp.vulnweb.com:80/.idea/.name
http://testphp.vulnweb.com:80/.idea
http://testphp.vulnweb.com:80/.idea/modules.xml
http://testphp.vulnweb.com:80/.idea/encodings.xml
http://testphp.vulnweb.com:80/.idea/workspace.xml
http://testphp.vulnweb.com:80/.idea/misc.xml
http://testphp.vulnweb.com:80/.idea/scopes/scope_settings.xml
http://testphp.vulnweb.com:80/.idea/vcs.xml
http://testphp.vulnweb.com:80/404.php
http://testphp.vulnweb.com:80/CVS/
http://testphp.vulnweb.com:80/CVS/Entries
http://testphp.vulnweb.com:80/CVS/Root
http://testphp.vulnweb.com:80/Connections
http://testphp.vulnweb.com:80/_mmServerScripts/
http://testphp.vulnweb.com:80/_mmServerScripts/MMHTTPDB.php
http://testphp.vulnweb.com:80/admin
http://testphp.vulnweb.com:80/admin/
http://testphp.vulnweb.com:80/admin/?/login
http://testphp.vulnweb.com:80/cart.php
http://testphp.vulnweb.com:80/cgi-bin/
http://testphp.vulnweb.com:80/cgi-bin
http://testphp.vulnweb.com:80/crossdomain.xml
http://testphp.vulnweb.com:80/favicon.ico
http://testphp.vulnweb.com:80/images
http://testphp.vulnweb.com:80/images/
http://testphp.vulnweb.com:80/index.php
http://testphp.vulnweb.com:80/index.bak
http://testphp.vulnweb.com:80/index.zip
http://testphp.vulnweb.com:80/login.php
http://testphp.vulnweb.com:80/logout.php
http://testphp.vulnweb.com:80/pictures
http://testphp.vulnweb.com:80/search.php
http://testphp.vulnweb.com:80/secured
http://testphp.vulnweb.com:80/signup.php
http://testphp.vulnweb.com:80/userinfo.php
```

### Save output in JSON format

JSON is an open standard file format and data exchange format that stores and transmits data objects consisting of attribute-value pairs and array data types using human-readable text. It is a very common data format with a wide variety of uses, such as being used in AJAX





systems as a substitute for XML. With this method, we can build this kind of output result format by just following these commands.

```
./dirsearch.py -u http://testphp.vulnweb.com/ --json-report=report
```

```
root@kali:~/dirsearch# ./dirsearch.py -u http://testphp.vulnweb.com/ --json-report=report
dirsearch v0.4.1
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10831
Error Log: /root/dirsearch/logs/errors-21-01-08_22-50-19.log
Target: http://testphp.vulnweb.com/
Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-08_22-50-20.txt
[22:50:20] Starting:
[22:50:32] 200 - 171B - /.idea/encodings.xml
[22:50:32] 200 - 275B - /.idea/modules.xml
[22:50:32] 200 - 266B - /.idea/misc.xml
[22:50:32] 301 - 169B - /.idea → http://testphp.vulnweb.com/.idea/
[22:50:32] 200 - 951B - /.idea/
[22:50:32] 200 - 6B - /.idea/.name
[22:50:32] 200 - 12KB - /.idea/workspace.xml
[22:50:32] 200 - 143B - /.idea/scopes/scope_settings.xml
[22:50:32] 200 - 173B - /.idea/vcs.xml
```

Similarly, as above we are using nano command to start analysing our result.

```
GNU nano 5.4 report
1
"http://testphp.vulnweb.com:80/": [
  {
    "content-length": 171,
    "path": "/.idea/encodings.xml",
    "redirect": null,
    "status": 200
  },
  {
    "content-length": 275,
    "path": "/.idea/modules.xml",
    "redirect": null,
    "status": 200
  },
  {
    "content-length": 266,
    "path": "/.idea/misc.xml",
    "redirect": null,
    "status": 200
  },
  {
    "content-length": 169,
    "path": "/.idea",
    "redirect": "http://testphp.vulnweb.com/.idea/",
    "status": 301
  },
  {
    "content-length": 951,
    "path": "/.idea/",
    "redirect": null,
    "status": 200
  },
  {
    "content-length": 6,
    "path": "/.idea/.name",
    "redirect": null,
    "status": 200
  },
  {
    "content-length": 12473,
    "path": "/.idea/workspace.xml",
    "redirect": null,
    "status": 200
  }
]
```



## Save output in XML format

Extensible Mark-up Language (XML) is a mark-up language that specifies a collection of rules that are both human-readable and machine-readable to encode documents in a format. By using some commands, we can build our XML format result copy with this tool.

```
./dirsearch.py -u http://testphp.vulnweb.com/ --xml-report=report
```

```
root@kali:~/dirsearch# ./dirsearch.py -u http://testphp.vulnweb.com/ --xml-report=report


clih-5 02-01-08

 v0.4.1

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10831
Error Log: /root/dirsearch/logs/errors-21-01-08_22-57-10.log
Target: http://testphp.vulnweb.com/
Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-08_22-57-11.txt

[22:57:11] Starting:
[22:57:23] 301 - 169B - /.idea → http://testphp.vulnweb.com/.idea/
[22:57:23] 200 - 951B - /.idea/
[22:57:24] 200 - 6B - /.idea/.name
[22:57:24] 200 - 171B - /.idea/encodings.xml
[22:57:24] 200 - 143B - /.idea/scopes/scope_settings.xml
```

Similarly, as above we are using nano command to start analysing our result.

```
GNU nano 5.4 report
<?xml version="1.0"?>
<time>Fri Jan 8 22:59:32 2021</time>
<target url="http://testphp.vulnweb.com:80/">
  <info path="/.idea">
    <status>301</status>
    <contentLength>169</contentLength>
    <redirect>http://testphp.vulnweb.com/.idea/</redirect>
  </info>
  <info path="/.idea/">
    <status>200</status>
    <contentLength>951</contentLength>
    <redirect>None</redirect>
  </info>
  <info path="/.idea/.name">
    <status>200</status>
    <contentLength>6</contentLength>
    <redirect>None</redirect>
  </info>
  <info path="/.idea/encodings.xml">
    <status>200</status>
    <contentLength>171</contentLength>
    <redirect>None</redirect>
  </info>
  <info path="/.idea/scopes/scope_settings.xml">
    <status>200</status>
    <contentLength>143</contentLength>
    <redirect>None</redirect>
  </info>
  <info path="/.idea/misc.xml">
    <status>200</status>
    <contentLength>266</contentLength>
    <redirect>None</redirect>
  </info>
  <info path="/.idea/modules.xml">
    <status>200</status>
    <contentLength>275</contentLength>
    <redirect>None</redirect>
  </info>
</target>
```



## Save output in Markdown format

For creating formatted text using a plain-text editor, Markdown is a lightweight mark-up language. In 2004, John Gruber and Aaron Swartz created Markdown as a mark-up language that, in its source code form, appeals to human readers. We can build our markdown format result copy by using this command with this tool.

```
./dirsearch.py -u http://testphp.vulnweb.com/ --markdown-report=report
```

```
root@kali:~/dirsearch# ./dirsearch.py -u http://testphp.vulnweb.com/ --markdown-report=report


d113 7211-ct
v0.4.1


Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10831
Error Log: /root/dirsearch/logs/errors-21-01-08_23-20-07.log
Target: http://testphp.vulnweb.com/
Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-08_23-20-08.txt
[23:20:08] Starting:
[23:20:22] 301 - 169B - /.idea → http://testphp.vulnweb.com/.idea/
[23:20:22] 200 - 951B - /.idea/
[23:20:23] 200 - 171B - /.idea/encodings.xml
[23:20:23] 200 - 6B - /.idea/name
```

Similarly, as above we are using nano command to start analysing our result.

```
GNU nano 5.4 report
## Time: Sat Jan 9 22:25:48 2021
## Target: http://testphp.vulnweb.com:80/

Path | Status | Size | Redirection
-----|-----|-----|-----
[/.idea](http://testphp.vulnweb.com:80/.idea) | 301 | 169 | http://testphp.vulnweb.c
[/.idea/](http://testphp.vulnweb.com:80/.idea/) | 200 | 951 | None
[/.idea/encodings.xml](http://testphp.vulnweb.com:80/.idea/encodings.xml) | 200 | 171 | None
[/.idea/.name](http://testphp.vulnweb.com:80/.idea/.name) | 200 | 6 | None
[/.idea/scopes/scope_settings.xml](http://testphp.vulnweb.com:80/.idea/scopes/scope_
[/.idea/modules.xml](http://testphp.vulnweb.com:80/.idea/modules.xml) | 200 | 275 | None
[/.idea/misc.xml](http://testphp.vulnweb.com:80/.idea/misc.xml) | 200 | 266 | None
[/.idea/vcs.xml](http://testphp.vulnweb.com:80/.idea/vcs.xml) | 200 | 173 | None
[/.idea/workspace.xml](http://testphp.vulnweb.com:80/.idea/workspace.xml) | 200 | 12
[/404.php](http://testphp.vulnweb.com:80/404.php) | 200 | 5268 | None
[/CVS/](http://testphp.vulnweb.com:80/CVS/) | 200 | 595 | None
[/CVS/Root](http://testphp.vulnweb.com:80/CVS/Root) | 200 | 1 | None
[/Connections](http://testphp.vulnweb.com:80/Connections) | 301 | 169 | http://testp
[/CVS/Entries](http://testphp.vulnweb.com:80/CVS/Entries) | 200 | 1 | None
[/_mmServerScripts/](http://testphp.vulnweb.com:80/_mmServerScripts/) | 200 | 400 | None
[/_mmServerScripts/MMHTTPDB.php](http://testphp.vulnweb.com:80/_mmServerScripts/MMHT
[/admin](http://testphp.vulnweb.com:80/admin) | 301 | 169 | http://testphp.vulnweb.c
[/admin/](http://testphp.vulnweb.com:80/admin/) | 200 | 262 | None
[/admin/?login](http://testphp.vulnweb.com:80/admin/?login) | 200 | 262 | None
[/cart.php](http://testphp.vulnweb.com:80/cart.php) | 200 | 4903 | None
[/cgi-bin](http://testphp.vulnweb.com:80/cgi-bin) | 403 | 276 | None
[/cgi-bin/](http://testphp.vulnweb.com:80/cgi-bin/) | 403 | 276 | None
[/crossdomain.xml](http://testphp.vulnweb.com:80/crossdomain.xml) | 200 | 224 | None
[/favicon.ico](http://testphp.vulnweb.com:80/favicon.ico) | 200 | 894 | None
[/images](http://testphp.vulnweb.com:80/images) | 301 | 169 | http://testphp.vulnweb
[/images/](http://testphp.vulnweb.com:80/images/) | 200 | 377 | None
[/index.php](http://testphp.vulnweb.com:80/index.php) | 200 | 4958 | None
[/index.bak](http://testphp.vulnweb.com:80/index.bak) | 200 | 3265 | None
[/index.zip](http://testphp.vulnweb.com:80/index.zip) | 200 | 2586 | None
[/login.php](http://testphp.vulnweb.com:80/login.php) | 200 | 5523 | None
[/logout.php](http://testphp.vulnweb.com:80/logout.php) | 200 | 4830 | None
[/pictures](http://testphp.vulnweb.com:80/pictures) | 301 | 169 | http://testphp.vul
[/search.php](http://testphp.vulnweb.com:80/search.php) | 200 | 4732 | None
[/secured](http://testphp.vulnweb.com:80/secured) | 301 | 169 | http://testphp.vulnw
[/signup.php](http://testphp.vulnweb.com:80/signup.php) | 200 | 6033 | None
[/userinfo.php](http://testphp.vulnweb.com:80/userinfo.php) | 302 | 14 | login.php
```



## Save Output in CSV format

A comma-separated value file is a delimited text file that separates values using a comma. A data record is any line of the file. Each record, separated by commas, consists of one or more fields. By using some commands, we can build our CSV result copy with this method.

```
./dirsearch.py -u http://testphp.vulnweb.com/ --csv-report=report
```

```
root@kali:~/dirsearch# ./dirsearch.py -u http://testphp.vulnweb.com/ --csv-report=report
v0.4.1
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10831
Error Log: /root/dirsearch/logs/errors-21-01-09_22-27-37.log
Target: http://testphp.vulnweb.com/
Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-09_22-27-37.txt
[22:27:37] Starting:
[22:27:42] 301 - 169B - /.idea → http://testphp.vulnweb.com/.idea/
[22:27:43] 200 - 951B - /.idea/
[22:27:43] 200 - 6B - /.idea/.name
```

Similarly, as above we are using nano command to start analysing our result.

```
GNU nano 5.4 report
time,URL,Status,Size,Redirection
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/.idea,301,169,"http://testphp.vulnweb.com:80/.idea/"
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/.idea/,200,951,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/.idea/.name,200,6,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/.idea/encodings.xml,200,171,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/.idea/misc.xml,200,266,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/.idea/modules.xml,200,275,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/.idea/scopes/scope_settings.xml,200,173,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/.idea/vcs.xml,200,173,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/.idea/workspace.xml,200,12473,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/404.php,200,5266,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/CVS/,200,595,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/CVS/Entries,200,1,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/CVS/Root,200,1,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/Connections,301,169,"http://testphp.vulnweb.com:80/_mmServerScripts/"
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/_mmServerScripts/MMHTTPDB.php,200,400,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/admin,301,169,"http://testphp.vulnweb.com:80/admin/"
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/admin/,200,262,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/admin/?/login,200,262,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/cart.php,200,4903,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/cgi-bin/,403,276,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/cgi-bin/,403,276,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/crossdomain.xml,200,224,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/favicon.ico,200,894,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/images/,200,377,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/images,301,169,"http://testphp.vulnweb.com:80/index.php"
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/index.php,200,4958,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/index.bak,200,3265,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/index.zip,200,2586,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/login.php,200,5523,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/logout.php,200,4830,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/pictures,301,169,"http://testphp.vulnweb.com:80/search.php"
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/search.php,200,4732,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/secured,301,169,"http://testphp.vulnweb.com:80/signup.php"
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/signup.php,200,6033,
Sat Jan 9 22:28:33 2021,http://testphp.vulnweb.com:80/userinfo.php,302,14,"login.php"
```



## Save output in Plain format

Simple text is a loose term for knowledge in computing that only represents characters of readable content, but not its graphical representation or other artefacts. It may also include a limited number of whitespace characters, such as spaces, line breaks, or tab characters, that affect the simple arrangement of text. By using some commands, we can create a plain text results copy with this method.

```
./dirsearch.py -u http://testphp.vulnweb.com/ --plain-text-report=report
```

```
root@kali:~/dirsearch# ./dirsearch.py -u http://testphp.vulnweb.com/ --plain-text-report=report
dirsearch v0.4.1
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10831
Error Log: /root/dirsearch/logs/errors-21-01-09_22-36-57.log
Target: http://testphp.vulnweb.com/
Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-09_22-36-57.txt
[22:36:57] Starting:
[22:37:02] 301 - 169B - /.idea → http://testphp.vulnweb.com/.idea/
[22:37:02] 200 - 951B - /.idea/
[22:37:02] 200 - 6B - /.idea/.name
```

Similarly, as above we are using nano command to start analysing our result.

```
GNU nano 5.4 report
Time: Sat Jan 9 22:37:02 2021
Time: Sat Jan 9 22:37:02 2021
301 169B http://testphp.vulnweb.com:80/.idea → REDIRECTS TO: http:
Time: Sat Jan 9 22:37:02 2021
Time: Sat Jan 9 22:37:02 2021
Time: Sat Jan 9 22:37:02 2021
200 951B http://testphp.vulnweb.com:80/.idea/
Time: Sat Jan 9 22:37:02 2021
Time: Sat Jan 9 22:37:02 2021
200 6B http://testphp.vulnweb.com:80/.idea/.name
Time: Sat Jan 9 22:37:02 2021
200 171B http://testphp.vulnweb.com:80/.idea/encodings.xml
Time: Sat Jan 9 22:37:02 2021
Time: Sat Jan 9 22:37:02 2021
200 266B http://testphp.vulnweb.com:80/.idea/misc.xml
Time: Sat Jan 9 22:37:02 2021
Time: Sat Jan 9 22:37:02 2021
200 275B http://testphp.vulnweb.com:80/.idea/modules.xml
Time: Sat Jan 9 22:37:02 2021
Time: Sat Jan 9 22:37:02 2021
200 143B http://testphp.vulnweb.com:80/.idea/scopes/scope_settings.xml
Time: Sat Jan 9 22:37:02 2021
Time: Sat Jan 9 22:37:02 2021
Time: Sat Jan 9 22:37:02 2021
200 173B http://testphp.vulnweb.com:80/.idea/vcs.xml
Time: Sat Jan 9 22:37:02 2021
200 12KB http://testphp.vulnweb.com:80/.idea/workspace.xml
Time: Sat Jan 9 22:37:07 2021
Time: Sat Jan 9 22:37:07 2021
200 5KB http://testphp.vulnweb.com:80/404.php
```



## No Colour

If colours are bothering us from concentrating on our analysis or results. We can remove all the colours occurs in our results from the attack, by using `[-no-colour]` parameter we can achieve this function. Follow this command to get these results.

```
./dirsearch.py -u http://testphp.vulnweb.com/ --no-color
```

```
root@kali:~/dirsearch# ./dirsearch.py -u http://testphp.vulnweb.com/ --no-color
v0.4.1
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10831
Error Log: /root/dirsearch/logs/errors-21-01-09_22-43-44.log
Target: http://testphp.vulnweb.com/
Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-09_22-43-45.txt
[22:43:45] Starting:
[22:43:50] 301 - 169B - /.idea → http://testphp.vulnweb.com/.idea/
[22:43:50] 200 - 951B - /.idea/
[22:43:50] 200 - 6B - /.idea/.name
[22:43:50] 200 - 171B - /.idea/encodings.xml
[22:43:50] 200 - 266B - /.idea/misc.xml
[22:43:50] 200 - 275B - /.idea/modules.xml
```

## Quite Mode

Quite mode is used in a more hush-hush manner to run dirsearch. If you're the type of person who doesn't want a huge banner telling everybody what you're doing on your system, you'll like this choice. Basically, this allows for a cleaner screen as it executes the commands you send it, without the funny cow showing up on top.

Just use this `[-q]` parameter with this command to see the results

```
./dirsearch.py -u http://testphp.vulnweb.com/ -q
```





```
root@kali:~/dirsearch# ./dirsearch.py -u http://testphp.vulnweb.com/ -q
301 - 169B - http://testphp.vulnweb.com/.idea → http://testphp.vulnweb.com/.idea/
200 - 951B - http://testphp.vulnweb.com/.idea/
200 - 171B - http://testphp.vulnweb.com/.idea/encodings.xml
200 - 6B - http://testphp.vulnweb.com/.idea/.name
200 - 266B - http://testphp.vulnweb.com/.idea/misc.xml
200 - 275B - http://testphp.vulnweb.com/.idea/modules.xml
200 - 143B - http://testphp.vulnweb.com/.idea/scopes/scope_settings.xml
200 - 173B - http://testphp.vulnweb.com/.idea/vcs.xml
200 - 12KB - http://testphp.vulnweb.com/.idea/workspace.xml
200 - 5KB - http://testphp.vulnweb.com/404.php
200 - 595B - http://testphp.vulnweb.com/ CVS/
200 - 1B - http://testphp.vulnweb.com/ CVS/Root
```

## Normal scan vs Recursive scan

The method of scanning everything in a folder, including subfolders, is known to all of us. We compare a normal scan against a recursive scan in this section.

Firstly, we only use the [-u] parameter in the normal scan to get through victim URLs. In order to begin this scan, follow this instruction.

```
./dirsearch.py -u http://testphp.vulnweb.com/
```



```
root@kali:~/dirsearch# ./dirsearch.py -u http://testphp.vulnweb.com/
dirsearch v0.4.1
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist: 31
Error Log: /root/dirsearch/logs/errors-21-01-13_12-34-55.log
Target: http://testphp.vulnweb.com/
Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-13_12-34-55.txt

[12:34:55] Starting:
[12:35:00] 301 - 169B - /.idea → http://testphp.vulnweb.com/.idea/
[12:35:00] 200 - 6B - /.idea/.name
[12:35:00] 200 - 951B - /.idea/
[12:35:00] 200 - 275B - /.idea/modules.xml
[12:35:00] 200 - 266B - /.idea/misc.xml
[12:35:00] 200 - 171B - /.idea/encodings.xml
[12:35:00] 200 - 143B - /.idea/scopes/scope_settings.xml
[12:35:01] 200 - 173B - /.idea/vcs.xml
[12:35:01] 200 - 12KB - /.idea/workspace.xml
[12:35:06] 200 - 5KB - /404.php
[12:35:07] 200 - 595B - /CVS/
[12:35:07] 200 - 1B - /CVS/Entries
[12:35:07] 200 - 1B - /CVS/Root
[12:35:07] 301 - 169B - /Connections → http://testphp.vulnweb.com/Connections
[12:35:12] 200 - 400B - /_mmServerScripts/
[12:35:12] 200 - 93B - /_mmServerScripts/MMHTTPDB.php
[12:35:14] 301 - 169B - /admin → http://testphp.vulnweb.com/admin/
[12:35:15] 200 - 262B - /admin/
[12:35:15] 200 - 262B - /admin/?/login
[12:35:27] 200 - 5KB - /cart.php
[12:35:27] 403 - 276B - /cgi-bin
[12:35:27] 403 - 276B - /cgi-bin/
[12:35:30] 200 - 224B - /crossdomain.xml
[12:35:34] 200 - 894B - /favicon.ico
[12:35:36] 301 - 169B - /images → http://testphp.vulnweb.com/images/
[12:35:36] 200 - 377B - /images/
[12:35:37] 200 - 5KB - /index.php
[12:35:37] 200 - 3KB - /index.bak
[12:35:37] 200 - 3KB - /index.zip
[12:35:40] 200 - 5KB - /login.php
[12:35:40] 200 - 5KB - /logout.php
[12:35:47] 301 - 169B - /pictures → http://testphp.vulnweb.com/pictures/
[12:35:50] 200 - 5KB - /search.php
[12:35:50] 301 - 169B - /secured → http://testphp.vulnweb.com/secured/
[12:35:52] 200 - 6KB - /signup.php
```

Now, secondly, in the same command, when we use the parameter [-r] along with it. By just initiating this attack on the victim, it will help us go through each folder and its sub folders.

```
./dirsearch.py -u http://testphp.vulnweb.com/ -r
```

As we can see these results, with specific wording, it attaches some more results, such as added to the queue in the ongoing attack.

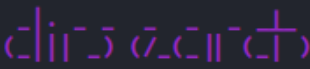




```
root@kali:~/dirsearch# ./dirsearch.py -u http://testphp.vulnweb.com/ -r


←



 v0.4.1

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 31

Error Log: /root/dirsearch/logs/errors-21-01-13_12-37-21.log

Target: http://testphp.vulnweb.com/

Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-13_12-37-22.txt

[12:37:22] Starting:
[12:37:27] 301 - 169B - /.idea → http://testphp.vulnweb.com/.idea/ (Added to queue)
[12:37:27] 200 - 951B - /.idea/
[12:37:27] 200 - 6B - /.idea/.name
[12:37:27] 200 - 266B - /.idea/misc.xml
[12:37:27] 200 - 171B - /.idea/encodings.xml
[12:37:27] 200 - 275B - /.idea/modules.xml
[12:37:27] 200 - 143B - /.idea/scopes/scope_settings.xml
[12:37:28] 200 - 173B - /.idea/vcs.xml
[12:37:28] 200 - 12KB - /.idea/workspace.xml
[12:37:33] 200 - 5KB - /404.php
[12:37:34] 200 - 595B - /CVS/ (Added to queue)
[12:37:34] 200 - 1B - /CVS/Root
[12:37:34] 200 - 1B - /CVS/Entries
[12:37:34] 301 - 169B - /Connections → http://testphp.vulnweb.com/Connections/ (Added to queue)
[12:37:39] 200 - 93B - /_mmServerScripts/MMHTTPODB.php
[12:37:39] 200 - 400B - /_mmServerScripts/ (Added to queue)
[12:37:44] 301 - 169B - /admin → http://testphp.vulnweb.com/admin/ (Added to queue)
[12:37:44] 200 - 262B - /admin/
[12:37:45] 200 - 262B - /admin?/login
[12:38:00] 200 - 5KB - /cart.php
[12:38:00] 403 - 276B - /cgi-bin/ (Added to queue)
[12:38:00] 403 - 276B - /cgi-bin
[12:38:04] 200 - 224B - /crossdomain.xml
[12:38:08] 200 - 894B - /favicon.ico
[12:38:11] 200 - 377B - /images/ (Added to queue)
[12:38:11] 301 - 169B - /images → http://testphp.vulnweb.com/images/
[12:38:12] 200 - 5KB - /index.php
[12:38:12] 200 - 3KB - /index.bak
[12:38:12] 200 - 3KB - /index.zip
[12:38:14] 200 - 5KB - /login.php
[12:38:15] 200 - 5KB - /logout.php
```

Now, after completing the usual scan for some time, it will go through each and every subfolder for the recursive scan. As we can see clearly in this screenshot, it goes for the victim's subfolders and tells us about our attack's incomplete work.



```
[12:56:34] 200 - 5KB - /login.php
[12:56:35] 200 - 5KB - /logout.php
[12:56:43] 301 - 169B - /pictures -> http://testphp.vulnweb.com/pictures/ (Added to queue)
[12:56:46] 200 - 5KB - /search.php
[12:56:46] 301 - 169B - /secured -> http://testphp.vulnweb.com/secured/ (Added to queue)
[12:56:47] 200 - 6KB - /signup.php
[12:56:53] 302 - 14B - /userinfo.php -> login.php
[12:56:57] Starting: .idea/
[12:57:04] 200 - 6B - /.idea/.name
[12:58:17] 200 - 12KB - /.idea/workspace.xml
[12:58:19] Starting: CVS/
[12:59:29] Starting: Connections/
[13:00:34] Starting: _mmServerScripts/
[13:01:26] 200 - 0B - /_mmServerScripts/mysql.php
[13:01:44] Starting: admin/
[13:02:48] Starting: cgi-bin/
[13:02:53] 403 - 276B - /cgi-bin/.ht_wsr.txt
[13:02:54] 403 - 276B - /cgi-bin/.htaccess.bak1
[13:02:54] 403 - 276B - /cgi-bin/.htaccess.orig
[13:02:54] 403 - 276B - /cgi-bin/.htaccess.save
[13:02:54] 403 - 276B - /cgi-bin/.htaccessBAK
[13:02:54] 403 - 276B - /cgi-bin/.htaccess.sample
[13:02:54] 403 - 276B - /cgi-bin/.htaccessOLD2
[13:02:54] 403 - 276B - /cgi-bin/.htaccessOLD
[13:02:54] 403 - 276B - /cgi-bin/.htm
[13:02:54] 403 - 276B - /cgi-bin/.htaccess_sc
[13:02:54] 403 - 276B - /cgi-bin/.html
[13:02:54] 403 - 276B - /cgi-bin/.htaccess_orig
[13:02:54] 403 - 276B - /cgi-bin/.htaccess_extra
[13:02:54] 403 - 276B - /cgi-bin/.htpasswd
[13:02:54] 403 - 276B - /cgi-bin/.htpasswd_test
[13:02:54] 403 - 276B - /cgi-bin/.http-oauth
[13:02:55] 403 - 276B - /cgi-bin/.php3
[13:03:01] 502 - 559B - /cgi-bin/CFIDE/administrator/ (Added to queue)
[13:03:01] 502 - 559B - /cgi-bin/CFIDE/Administrator/startstop.html
[13:03:01] 502 - 559B - /cgi-bin/CHANGELOG
[13:03:01] 502 - 559B - /cgi-bin/CFIDE/scripts/ajax/FCKeditor
[13:03:01] 502 - 559B - /cgi-bin/CHANGELOG.log
[13:03:01] 502 - 559B - /cgi-bin/CHANGELOG.html
[13:03:01] 502 - 559B - /cgi-bin/CHANGELOG.HTML
[13:03:01] 502 - 559B - /cgi-bin/CHANGELOG.TXT
[13:03:01] 502 - 559B - /cgi-bin/CHANGELOG.MD
16.94% - Job: 7/11 - Last request to: Estadisticas/
```

## Post method

We know that, for a given resource, HTTP defines a set of request methods to indicate the required action to be performed.

But in the post method, POST is an HTTP supported request method used by the World Wide Web. The POST request method, by design, requires a web server to accept the data enclosed in the request message body, most likely to store it. It normally works with the GET HTTP method, which is used in the name or value pair to append the form data to the URL. If you use GET, the URL length will remain restricted. This enables users to submit the result of the bookmark.

Now, we are exploring this other side with the help of [-m] parameter with this command.



As we can these results are different and unique in comparison to the GET request method which we performed earlier. It shows some different web pages and web directories.

```
./dirsearch.py -u http://testphp.vulnweb.com/ -m POST
```

```
root@kali:~/dirsearch# ./dirsearch.py -u http://testphp.vulnweb.com/ -m POST
dirsearch v0.4.1
Extensions: php, aspx, jsp, html, js | HTTP method: POST | Threads: 30 | Wordlist:
Error Log: /root/dirsearch/logs/errors-21-01-13_13-04-21.log
Target: http://testphp.vulnweb.com/
Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-13_13-04-21.txt

[13:04:21] Starting:
[13:04:30] 301 - 169B - /.idea → http://testphp.vulnweb.com/.idea/
[13:04:30] 405 - 559B - /.idea/.name
[13:04:30] 403 - 555B - /.idea/
[13:04:30] 405 - 559B - /.idea/modules.xml
[13:04:30] 405 - 559B - /.idea/misc.xml
[13:04:30] 405 - 559B - /.idea/encodings.xml
[13:04:30] 405 - 559B - /.idea/scopes/scope_settings.xml
[13:04:30] 405 - 559B - /.idea/vcs.xml
[13:04:30] 405 - 559B - /.idea/workspace.xml
[13:04:35] 200 - 5KB - /404.php
[13:04:36] 405 - 559B - /CVS/Root
[13:04:36] 405 - 559B - /CVS/Entries
[13:04:36] 403 - 555B - /CVS/
[13:04:36] 301 - 169B - /Connections → http://testphp.vulnweb.com/Connections/
[13:04:41] 200 - 93B - /_mmServerScripts/MMHTTPDB.php
[13:04:41] 403 - 555B - /_mmServerScripts/
[13:04:43] 301 - 169B - /admin → http://testphp.vulnweb.com/admin/
[13:04:44] 403 - 555B - /admin/
[13:04:44] 403 - 555B - /admin/?/login
[13:04:56] 200 - 5KB - /cart.php
[13:04:56] 403 - 276B - /cgi-bin
[13:04:56] 403 - 276B - /cgi-bin/
[13:04:59] 405 - 559B - /crossdomain.xml
[13:05:03] 405 - 559B - /favicon.ico
[13:05:05] 301 - 169B - /images → http://testphp.vulnweb.com/images/
[13:05:05] 403 - 555B - /images/
[13:05:06] 200 - 5KB - /index.php
[13:05:06] 405 - 559B - /index.bak
[13:05:06] 405 - 559B - /index.zip
[13:05:09] 200 - 5KB - /login.php
[13:05:09] 200 - 5KB - /logout.php
[13:05:16] 301 - 169B - /pictures → http://testphp.vulnweb.com/pictures/
[13:05:19] 200 - 5KB - /search.php
[13:05:19] 301 - 169B - /secured → http://testphp.vulnweb.com/secured/
[13:05:21] 200 - 6KB - /signup.php
[13:05:25] 302 - 14B - /userinfo.php → login.php
```



## Delay request

It just another normal scan with some specific delay between each and every request in our attack. These sorts of things provide proper exposure of a particular request. We can achieve this feature with the help of [-s] parameter with specified time in seconds.

```
./dirsearch.py -u http://testphp.vulnweb.com/ -s 10
```

```
root@kali:~/dirsearch# ./dirsearch.py -u http://testphp.vulnweb.com/ -s 10
dirsearch v0.4.1
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10
Error Log: /root/dirsearch/logs/errors-21-01-13_13-14-38.log
Target: http://testphp.vulnweb.com/
Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-13_13-14-39.txt

[13:14:39] Starting:
[13:18:17] 301 - 169B - /.idea → http://testphp.vulnweb.com/.idea/
[13:18:17] 200 - 6B - /.idea/.name
[13:18:17] 200 - 951B - /.idea/
[13:18:26] 200 - 171B - /.idea/encodings.xml
[13:18:26] 200 - 275B - /.idea/modules.xml
[13:18:26] 200 - 266B - /.idea/misc.xml
[13:18:27] 200 - 143B - /.idea/scopes/scope_settings.xml
[13:18:27] 200 - 173B - /.idea/vcs.xml
[13:18:28] 200 - 12KB - /.idea/workspace.xml
[13:23:23] 200 - 5KB - /404.php
[13:24:43] 200 - 595B - /CVS/
[13:24:43] 200 - 1B - /CVS/Entries
[13:24:43] 200 - 1B - /CVS/Root
[13:24:53] 301 - 169B - /Connections → http://testphp.vulnweb.com/Connections/
22.99% - Last request to: _function/
```



## Version scan

As we all know that our dirsearch web content scanner is constantly being updating with the time. Some feature will add in the with the demand of time. We can use [-version] parameter to see that, if our tool is up to date or not.

```
./dirsearch.py --version
```

```
root@kali:~/dirsearch# ./dirsearch.py --version  
dirsearch v0.4.1
```

## Conclusion

This marks the end of the Dirsearch Guide, focusing on some of Dirsearch's main features.

Hence, one can make use of these commands as a cybersecurity professional to assess vulnerabilities on systems and keep these systems away from threat.

## References

- <https://www.hackingarticles.in/comprehensive-guide-on-dirsearch/>
- <https://github.com/shelld3v>
- <https://github.com/maurosoria/dirsearch.git>