DirBuster

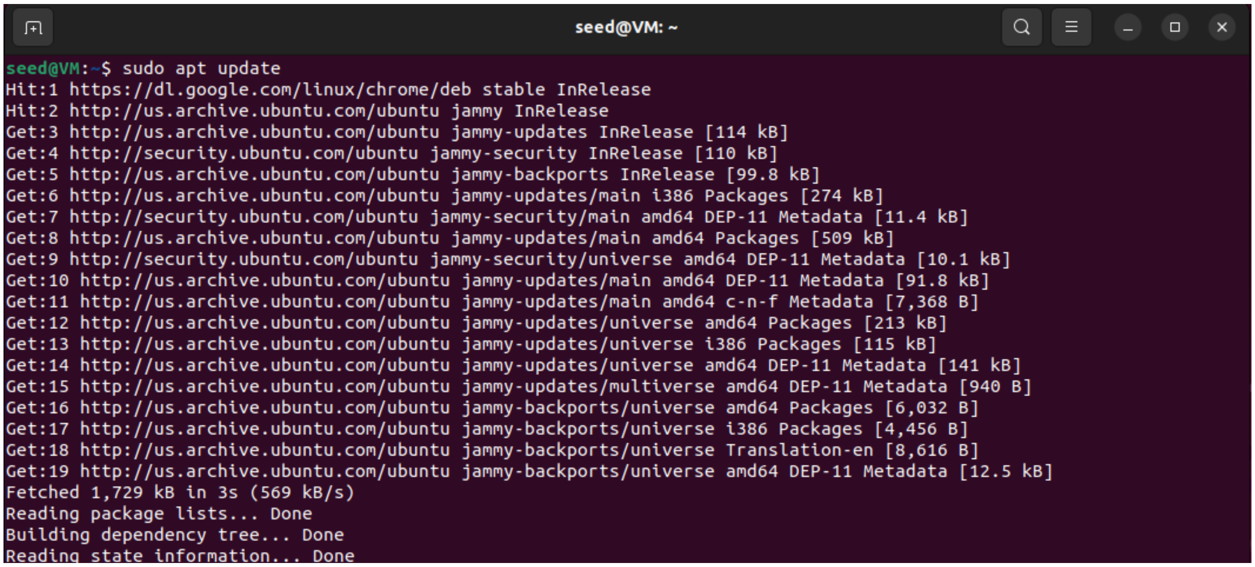
DirBuster is a multi-threaded Java application that brute forces directory and file names on web/application servers. What appears to be a web server in its default configuration is frequently not, and has pages and applications hidden within. DirBuster makes an attempt to locate these.

Installation:

The tool is preinstalled on Kali Linux OS but for this exercise Ubuntu 20.04 machine is used. On any Linux distribution this tool can be installed using following steps:

Step 1: Install apt updates using following command

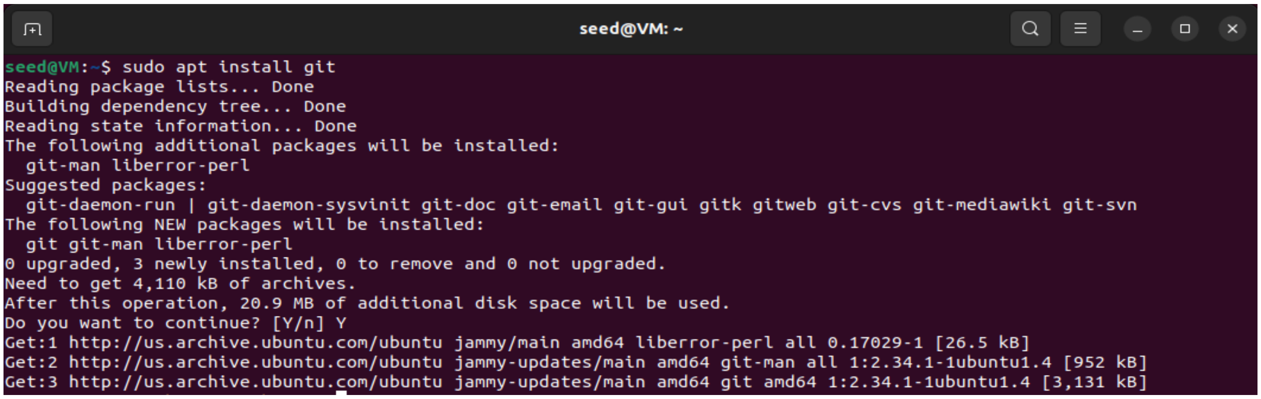
- sudo apt update



```
seed@VM:~$ sudo apt update
Hit:1 https://dl.google.com/linux/chrome/deb stable InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu jammy InRelease
Get:3 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease [114 kB]
Get:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease [99.8 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu jammy-updates/main i386 Packages [274 kB]
Get:7 http://security.ubuntu.com/ubuntu jammy-security/main amd64 DEP-11 Metadata [11.4 kB]
Get:8 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [509 kB]
Get:9 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 DEP-11 Metadata [10.1 kB]
Get:10 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 DEP-11 Metadata [91.8 kB]
Get:11 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [7,368 B]
Get:12 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [213 kB]
Get:13 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe i386 Packages [115 kB]
Get:14 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 DEP-11 Metadata [141 kB]
Get:15 http://us.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 DEP-11 Metadata [940 B]
Get:16 http://us.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 Packages [6,032 B]
Get:17 http://us.archive.ubuntu.com/ubuntu jammy-backports/universe i386 Packages [4,456 B]
Get:18 http://us.archive.ubuntu.com/ubuntu jammy-backports/universe Translation-en [8,616 B]
Get:19 http://us.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 DEP-11 Metadata [12.5 kB]
Fetched 1,729 kB in 3s (569 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

Step 2: After updating the packages, next step is to install Git using following command

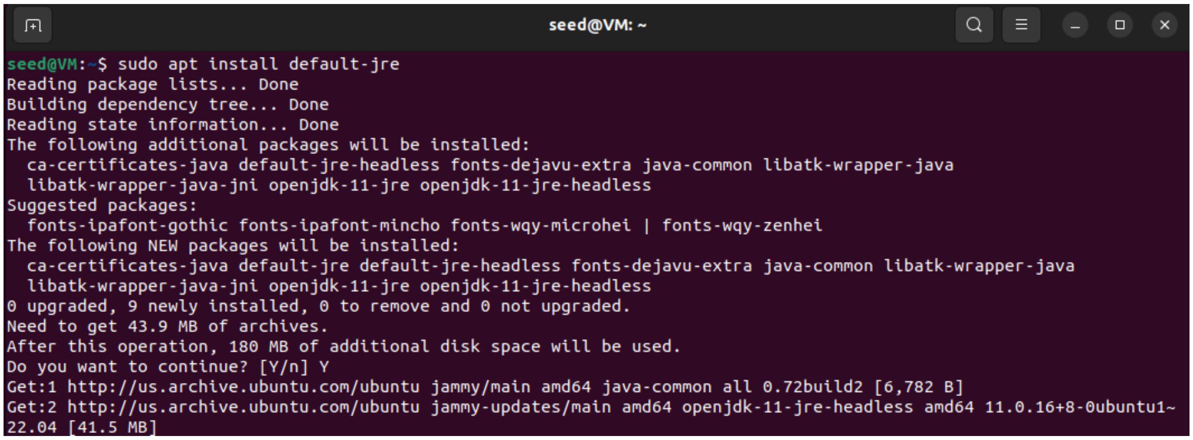
- sudo apt install git



```
seed@VM:~$ sudo apt install git
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  git-man liberror-perl
Suggested packages:
  git-daemon-run | git-daemon-sysvinit git-doc git-email git-gui gitk gitweb git-cvs git-mediawiki git-svn
The following NEW packages will be installed:
  git git-man liberror-perl
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 4,110 kB of archives.
After this operation, 20.9 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://us.archive.ubuntu.com/ubuntu jammy/main amd64 liberror-perl all 0.17029-1 [26.5 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 git-man all 1:2.34.1-1ubuntu1.4 [952 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 git amd64 1:2.34.1-1ubuntu1.4 [3,131 kB]
```

Step 3: Next step is to check and installed latest Java version

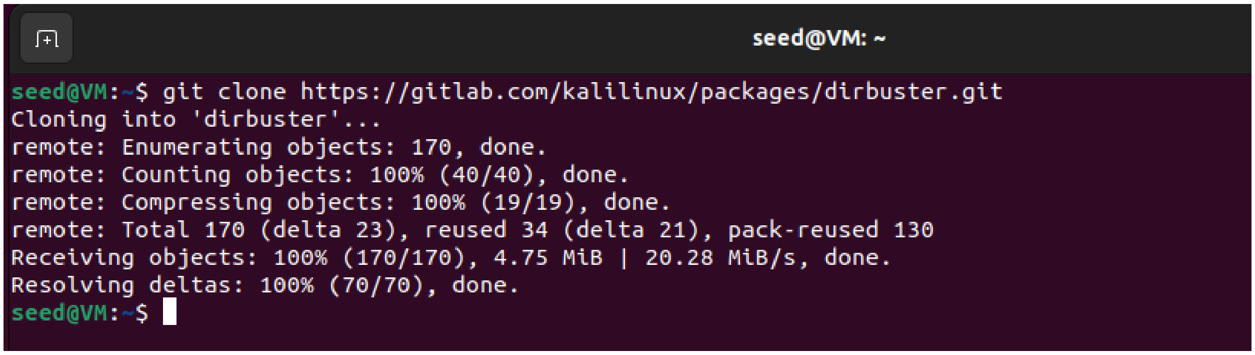
- sudo apt install default-jre



```
seed@VM:~$ sudo apt install default-jre
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ca-certificates-java default-jre-headless fonts-dejavu-extra java-common libatk-wrapper-java
  libatk-wrapper-java-jni openjdk-11-jre openjdk-11-jre-headless
Suggested packages:
  fonts-ipafont-gothic fonts-ipafont-mincho fonts-wqy-microhei | fonts-wqy-zenhei
The following NEW packages will be installed:
  ca-certificates-java default-jre default-jre-headless fonts-dejavu-extra java-common libatk-wrapper-java
  libatk-wrapper-java-jni openjdk-11-jre openjdk-11-jre-headless
0 upgraded, 9 newly installed, 0 to remove and 0 not upgraded.
Need to get 43.9 MB of archives.
After this operation, 180 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://us.archive.ubuntu.com/ubuntu jammy/main amd64 java-common all 0.72build2 [6,782 B]
Get:2 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openjdk-11-jre-headless amd64 11.0.16+8-0ubuntu1~
22.04 [41.5 MB]
```

Step 4: After installing the prerequisites, next step is to clone DirBuster git repository and move it to opt directory which is done using following commands:

- git clone https://gitlab.com/kalilinux/packages/dirbuster.git

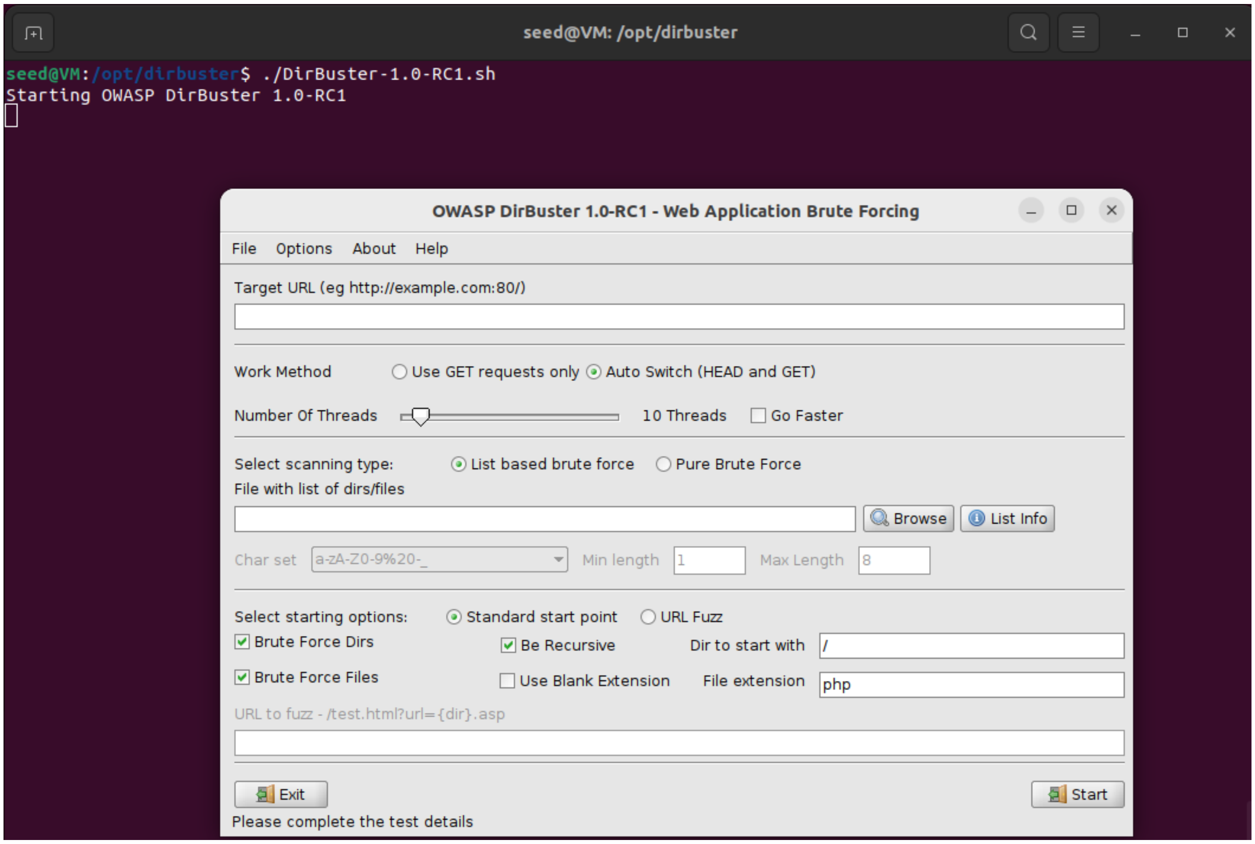


```
seed@VM:~$ git clone https://gitlab.com/kalilinux/packages/dirbuster.git
Cloning into 'dirbuster'...
remote: Enumerating objects: 170, done.
remote: Counting objects: 100% (40/40), done.
remote: Compressing objects: 100% (19/19), done.
remote: Total 170 (delta 23), reused 34 (delta 21), pack-reused 130
Receiving objects: 100% (170/170), 4.75 MiB | 20.28 MiB/s, done.
Resolving deltas: 100% (70/70), done.
seed@VM:~$
```

- sudo mv dirbuster /opt

Step 5: After running above command, it is possible to run the tool using following command and various options within in it can be toggled using GUI as shown below:

- ./DirBuster-1.0-RC1.sh



```
seed@VM:/opt/dirbuster$ ./DirBuster-1.0-RC1.sh
Starting OWASP DirBuster 1.0-RC1
```

Target URL (eg http://example.com:80/)

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 10 Threads □ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

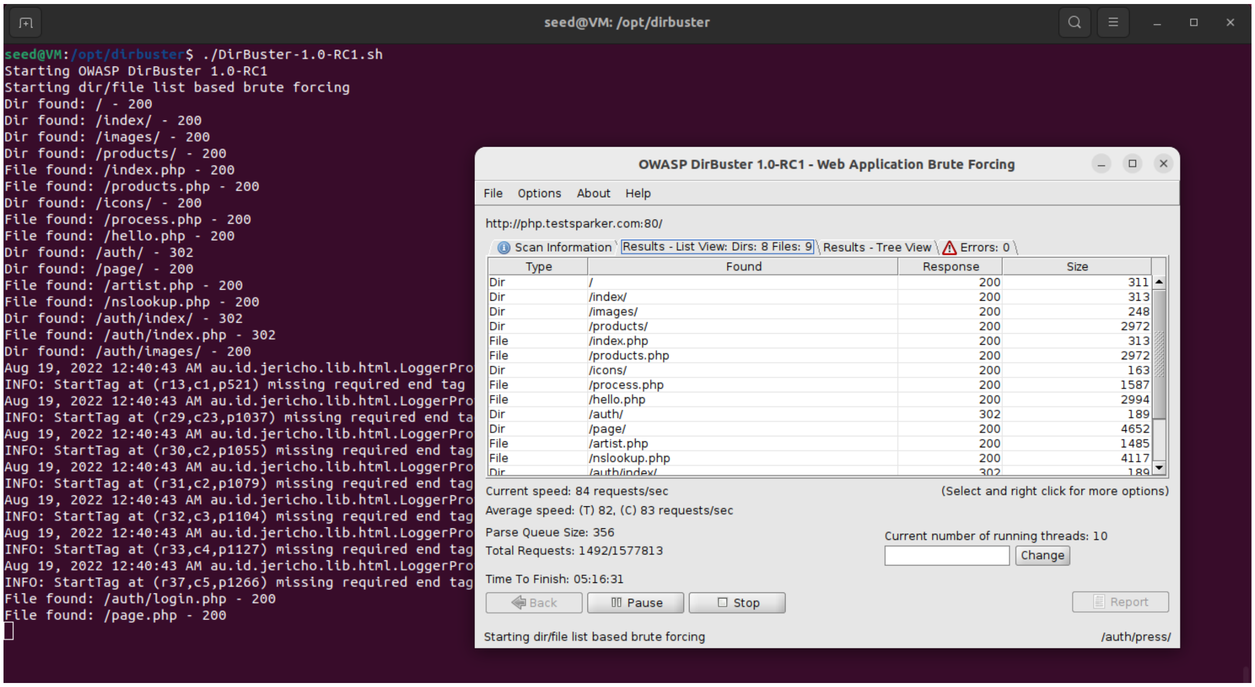
☑ Brute Force Files □ Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp

Please complete the test details

Execution:

After installing the tool, for this guide the tool will be run against following demo vulnerable website to bruteforce and identify hidden directories as shown in below screenshot using default available directory list available within the tool:



```
seed@VM:/opt/dirbuster$ ./DirBuster-1.0-RC1.sh
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
Dir found: / - 200
Dir found: /index/ - 200
Dir found: /images/ - 200
Dir found: /products/ - 200
File found: /index.php - 200
File found: /products.php - 200
Dir found: /icons/ - 200
File found: /process.php - 200
File found: /hello.php - 200
Dir found: /auth/ - 302
Dir found: /page/ - 200
File found: /artist.php - 200
File found: /nslookup.php - 200
Dir found: /auth/index/ - 302
File found: /auth/index.php - 302
Dir found: /auth/images/ - 200
Aug 19, 2022 12:40:43 AM au.id.jericho.lib.html.LoggerPro
INFO: StartTag at (r13,c1,p521) missing required end tag
Aug 19, 2022 12:40:43 AM au.id.jericho.lib.html.LoggerPro
INFO: StartTag at (r29,c23,p1037) missing required end ta
Aug 19, 2022 12:40:43 AM au.id.jericho.lib.html.LoggerPro
INFO: StartTag at (r30,c2,p1055) missing required end tag
Aug 19, 2022 12:40:43 AM au.id.jericho.lib.html.LoggerPro
INFO: StartTag at (r31,c2,p1079) missing required end tag
Aug 19, 2022 12:40:43 AM au.id.jericho.lib.html.LoggerPro
INFO: StartTag at (r32,c3,p1104) missing required end tag
Aug 19, 2022 12:40:43 AM au.id.jericho.lib.html.LoggerPro
INFO: StartTag at (r33,c4,p1127) missing required end tag
Aug 19, 2022 12:40:43 AM au.id.jericho.lib.html.LoggerPro
INFO: StartTag at (r37,c5,p1266) missing required end tag
File found: /auth/login.php - 200
File found: /page.php - 200
```

http://php.testsparker.com:80/

Type	Found	Response	Size
Dir	/	200	311
Dir	/index/	200	313
Dir	/images/	200	248
Dir	/products/	200	2972
File	/index.php	200	313
File	/products.php	200	2972
Dir	/icons/	200	163
File	/process.php	200	1587
File	/hello.php	200	2994
Dir	/auth/	302	189
Dir	/page/	200	4652
File	/artist.php	200	1485
File	/nslookup.php	200	4117
Dir	/auth/index/	302	189

Current speed: 84 requests/sec
(Select and right click for more options)
Average speed: (T) 82, (C) 83 requests/sec
Parse Queue Size: 356
Total Requests: 1492/1577813
Current number of running threads: 10
Time To Finish: 05:16:31

Starting dir/file list based brute forcing
/auth/press/

As observed, the tool is successfully bruteforce the directories available within the vulnerable web application. Like this example, this tool can be used in actual ethical penetration test to perform scan against the target domain to identify and find if any sensitive information is exposed by traversing through directories.