

[illegible]

Name	Directory Enumeration with Dirbuster
URL	https://attackdefense.com/challengedetails?cid=1883
Type	Webapp Pentesting Basics

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Perform directory enumeration with Dirbuster

Solution:

Step 1: Start a terminal and check the IP address of the host.

Command: ip addr

```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
24861: eth0@if24862: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:05 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.5/24 brd 10.1.1.255 scope global eth0
        valid_lft forever preferred_lft forever
24864: eth1@if24865: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:9c:cf:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.156.207.2/24 brd 192.156.207.255 scope global eth1
        valid_lft forever preferred_lft forever
root@attackdefense:~#
```

Step 2: Run Nmap scan on the target IP to find open ports.

Note: The target IP will be 192.156.207.3

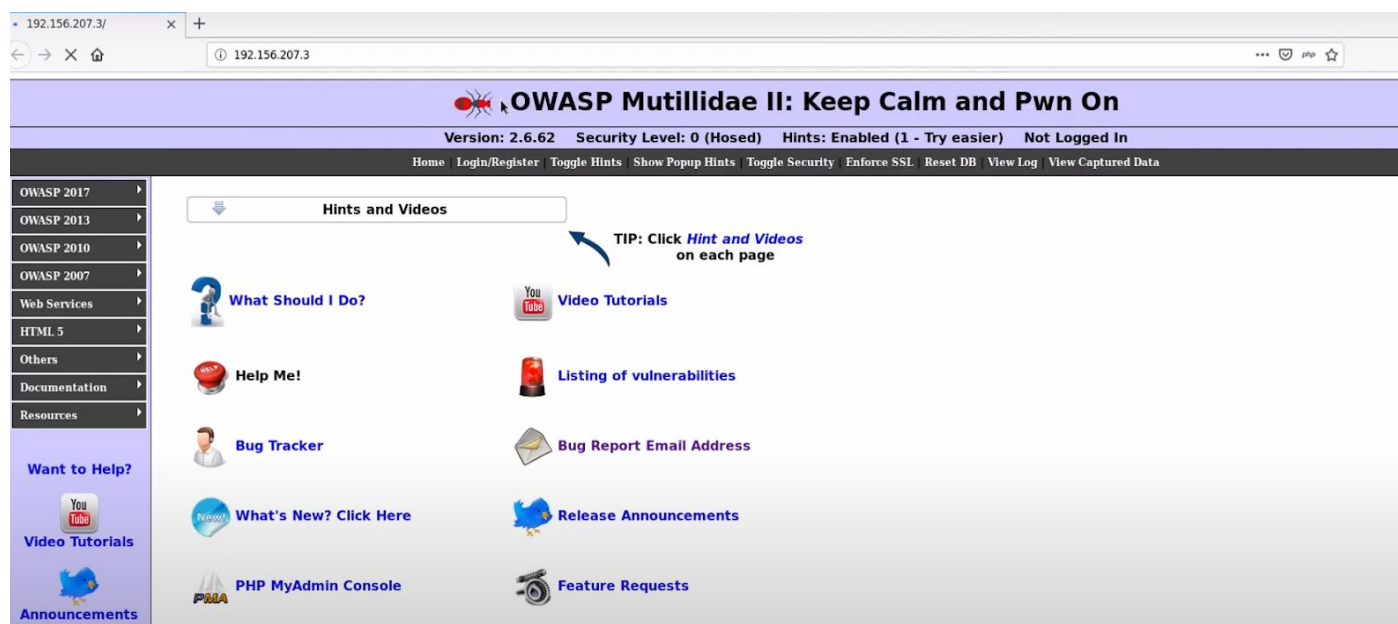
Command: nmap 192.156.207.3

```
root@attackdefense:~# nmap 192.156.207.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-19 18:57 IST
Nmap scan report for target-1 (192.156.207.3)
Host is up (0.000013s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 02:42:C0:9C:CF:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
root@attackdefense:~#
```

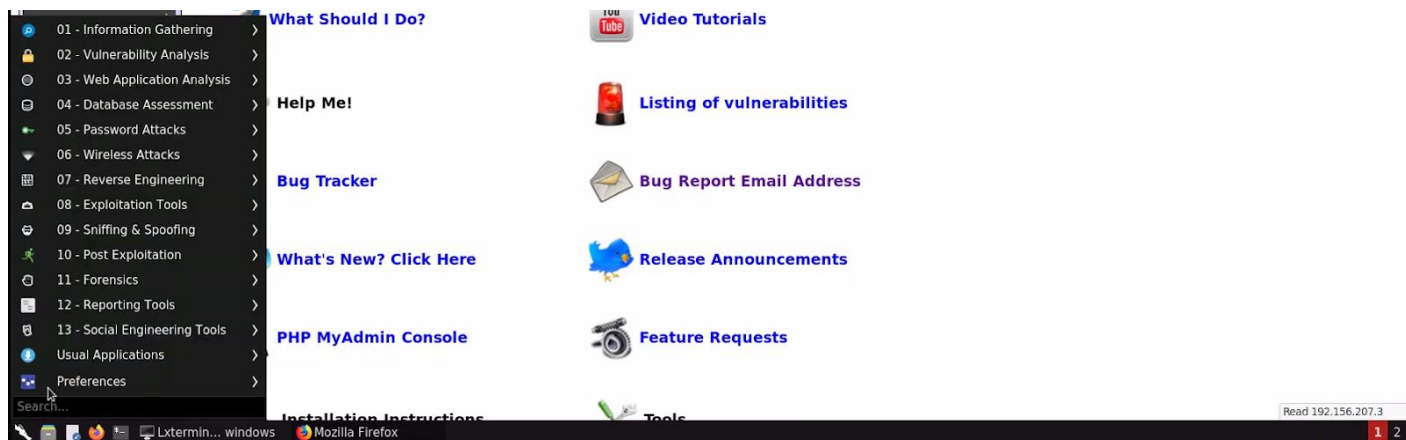
Port 80 and Port 3306 are open

Step 3: Start firefox and navigate to the target IP.

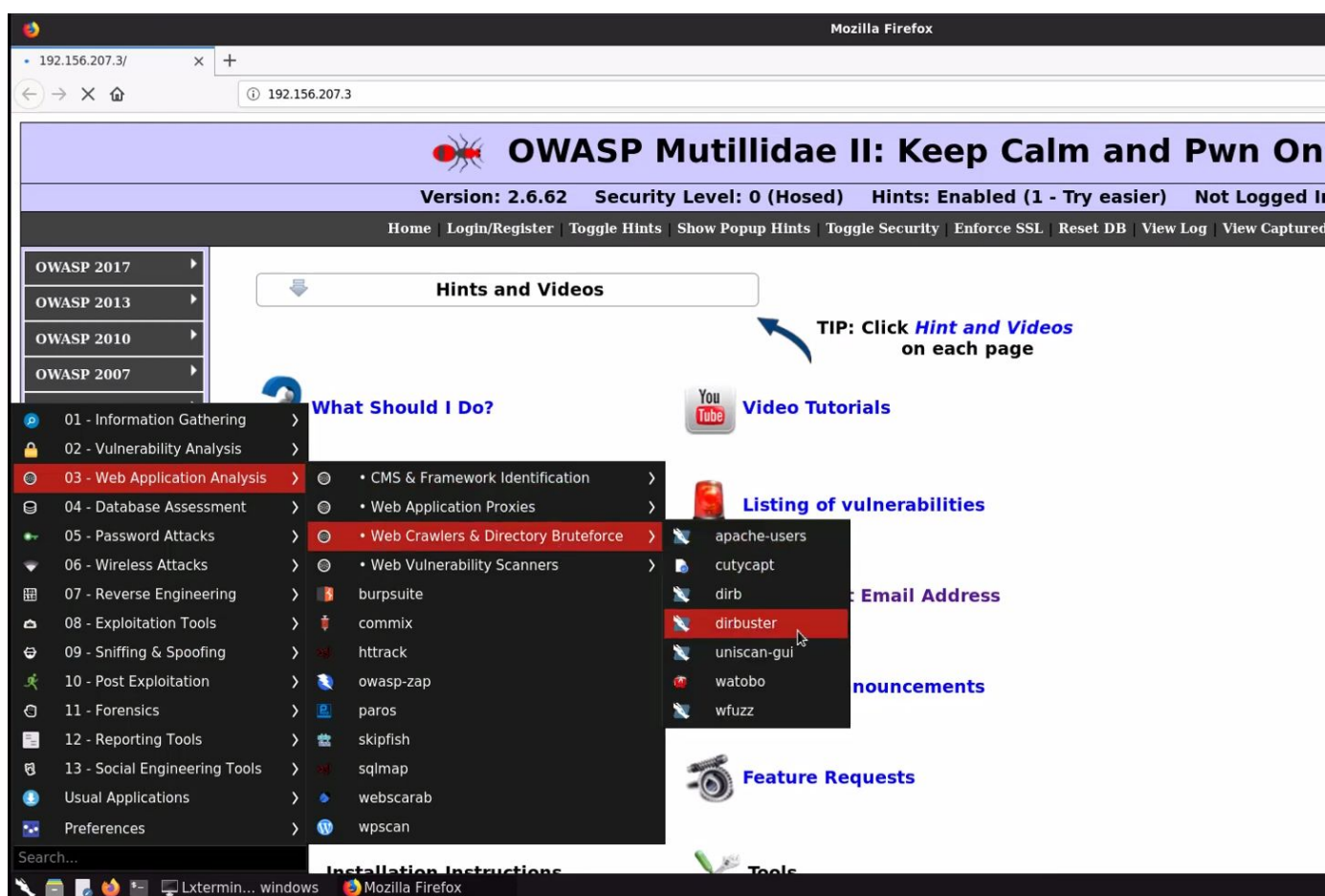


An instance of Mutillidae is running at port 80 of the target.

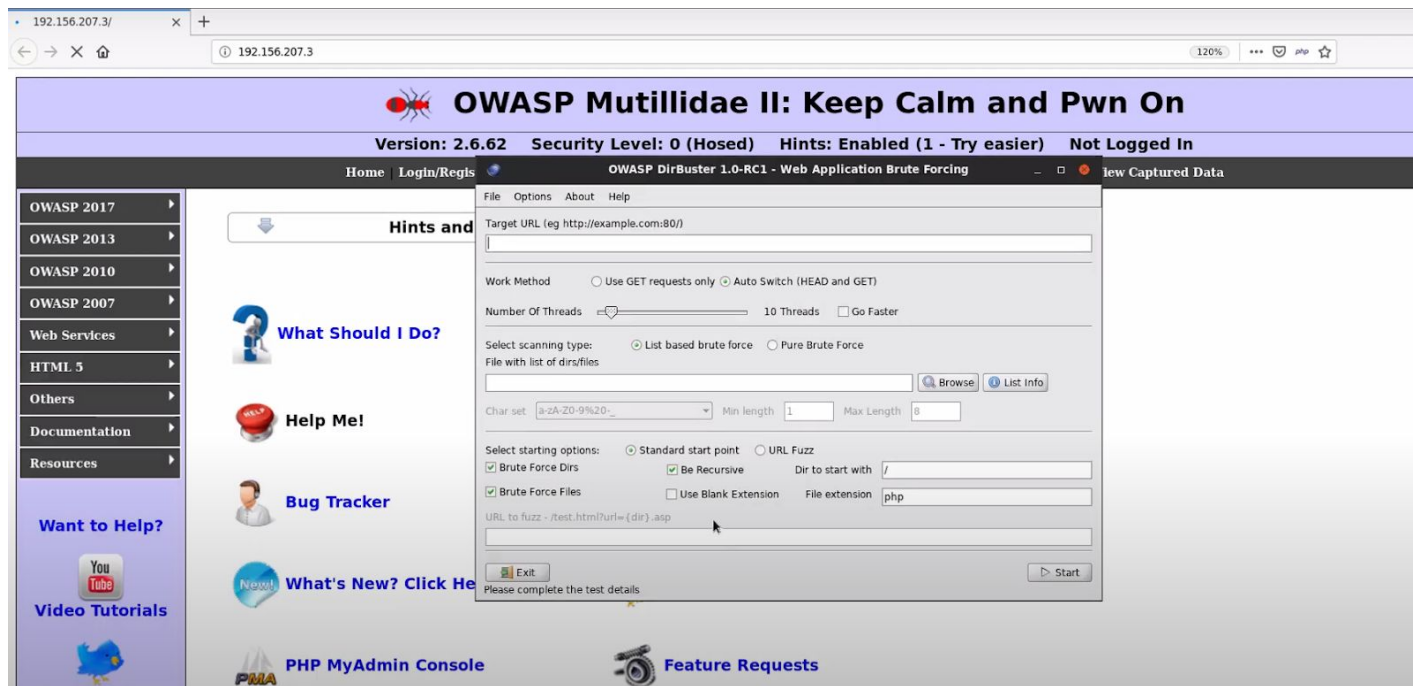
Step 4: Click on the menu (start) button.



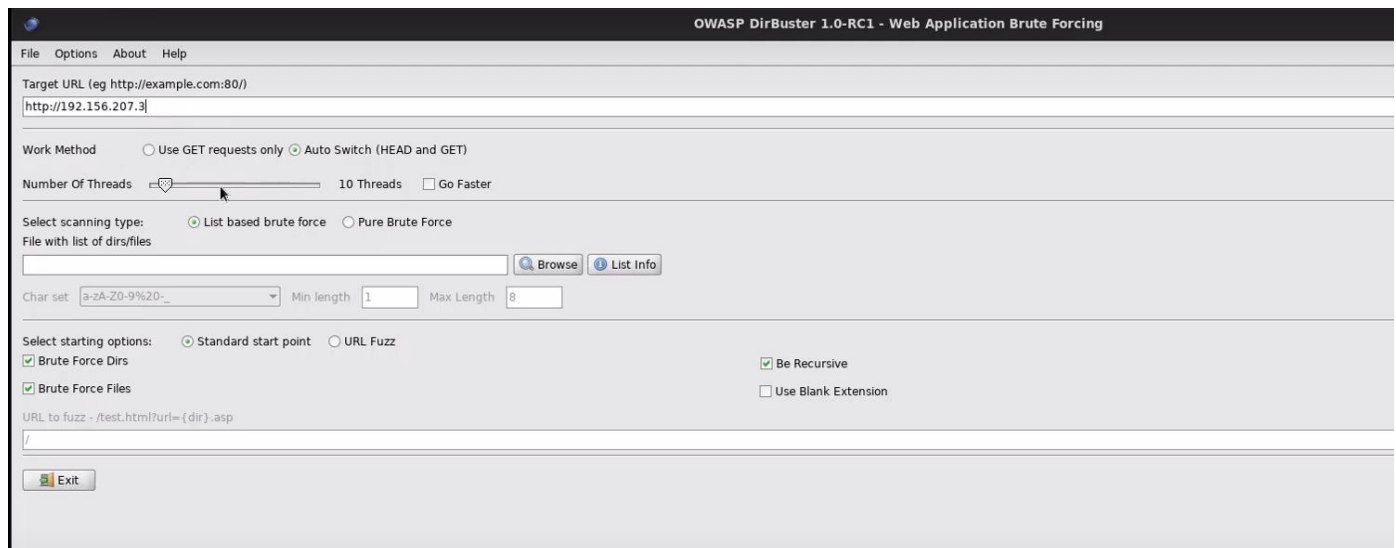
Navigate to Web application Analysis then Web Crawlers & Directory Bruteforce



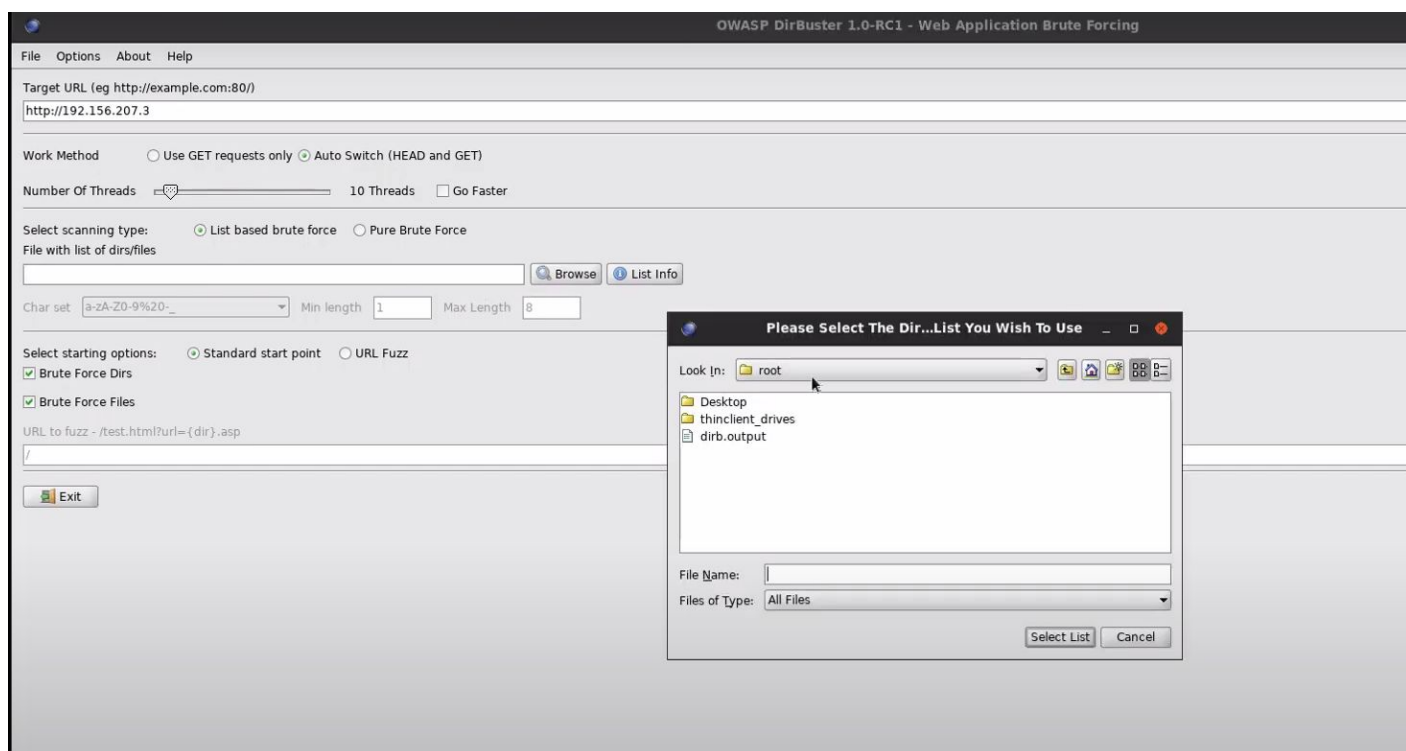
Click on “dirbuster”.



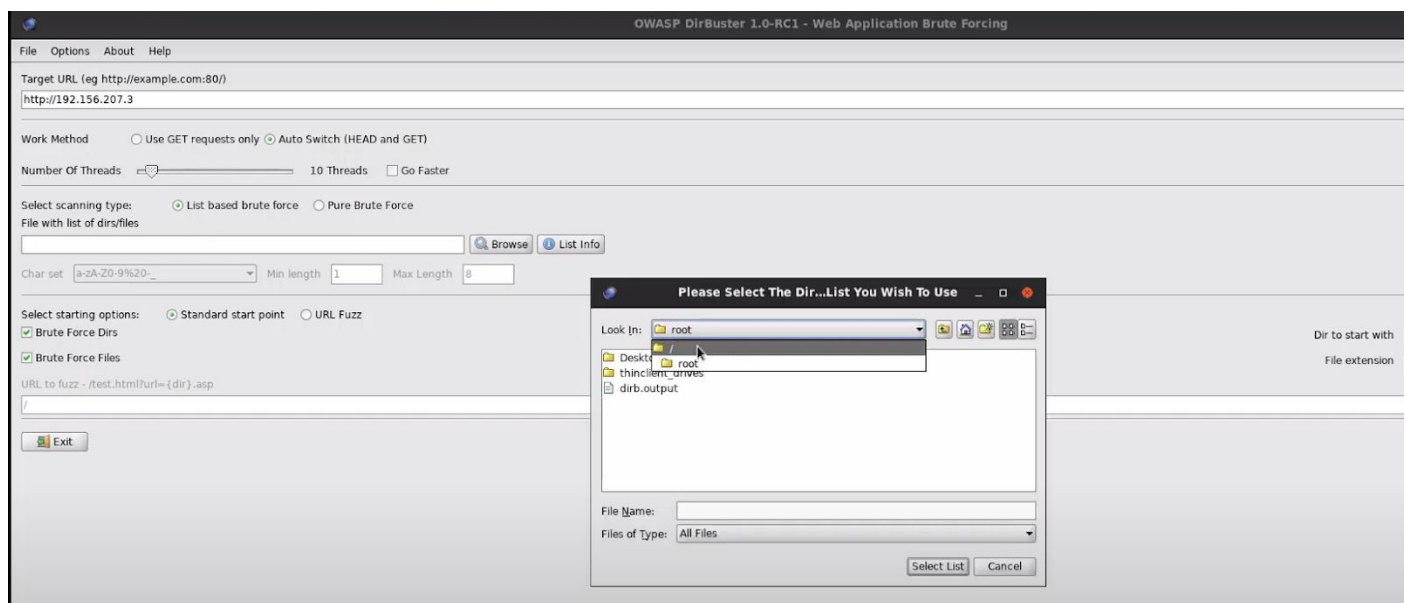
Step 5: Enter the target URL and select “Auto Switch” in Work Method



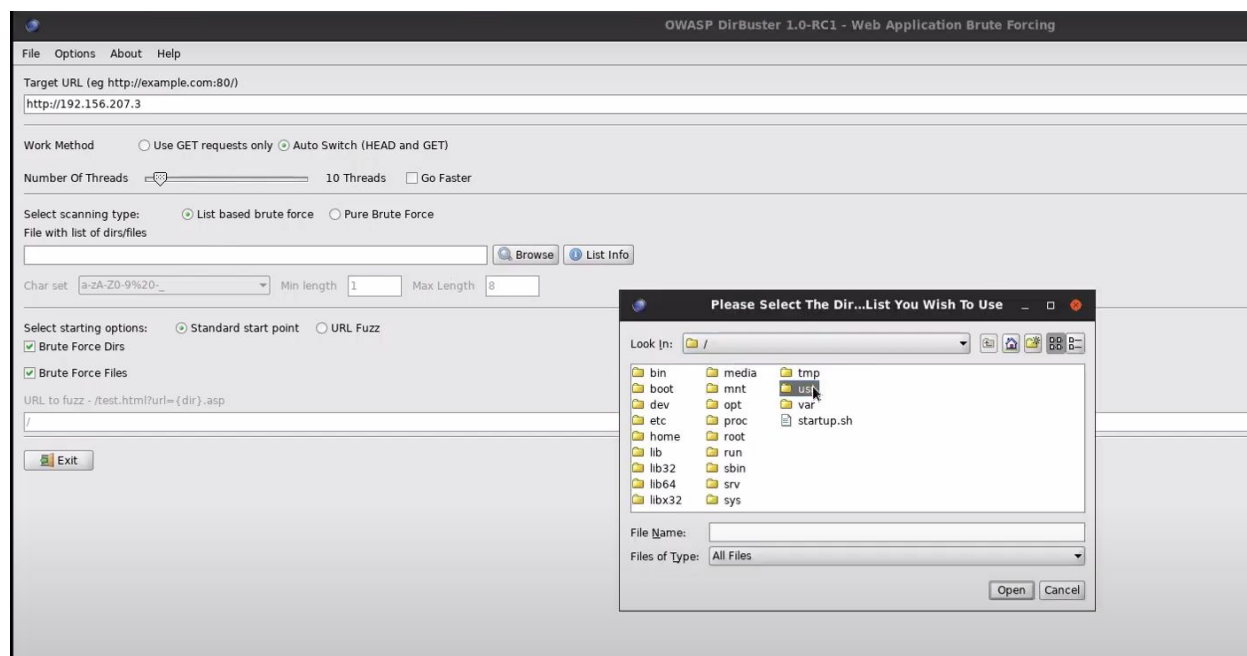
Click on the “Browse” button to select the wordlist.



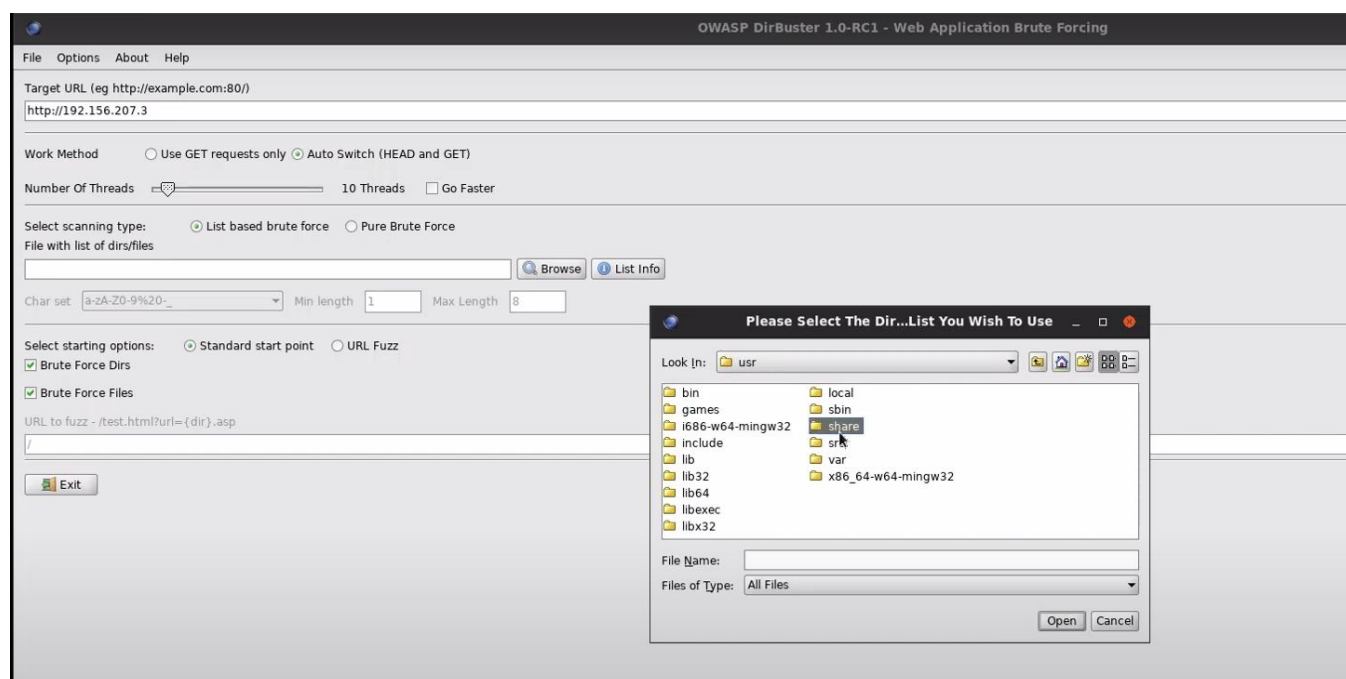
Click on the drop-down menu and choose the root directory (/)



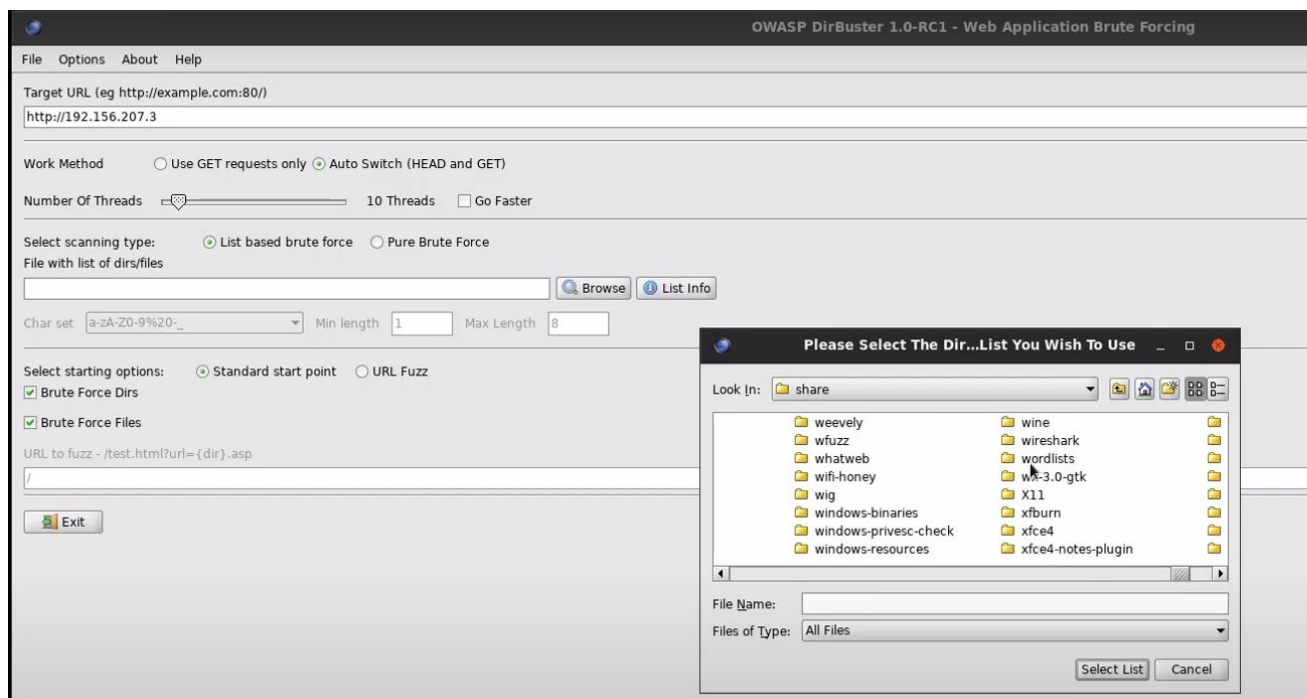
Choose the “usr” directory.



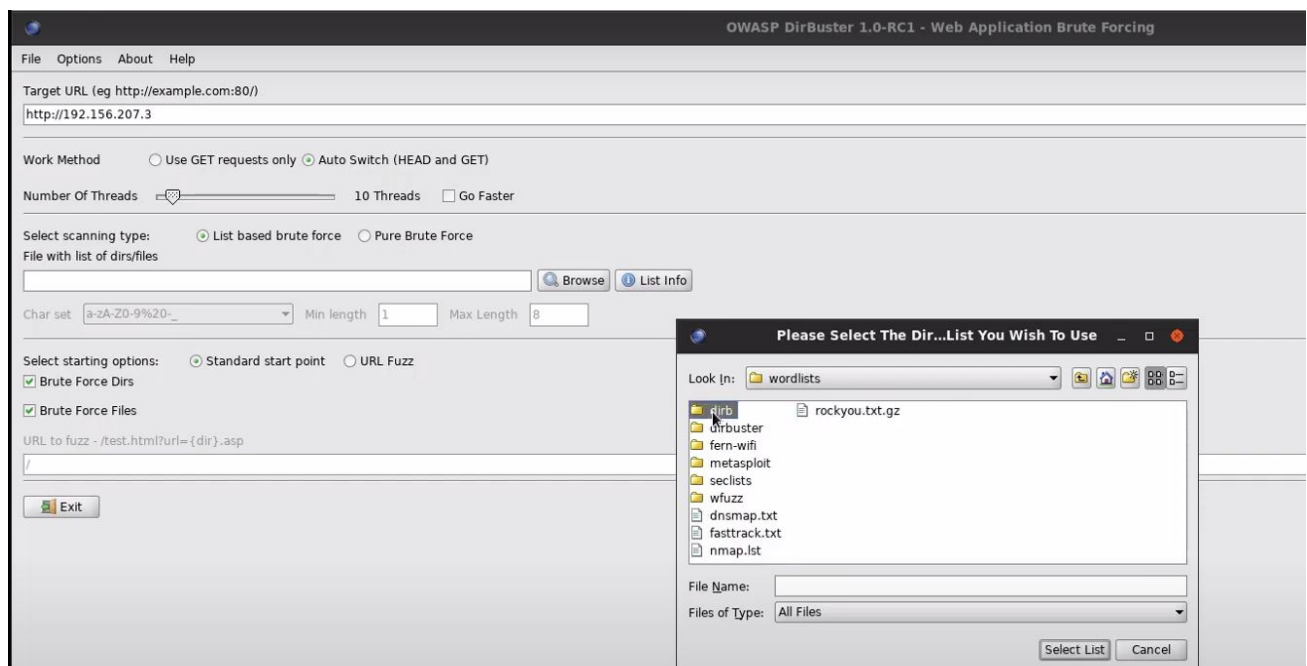
Click on the “share” directory.



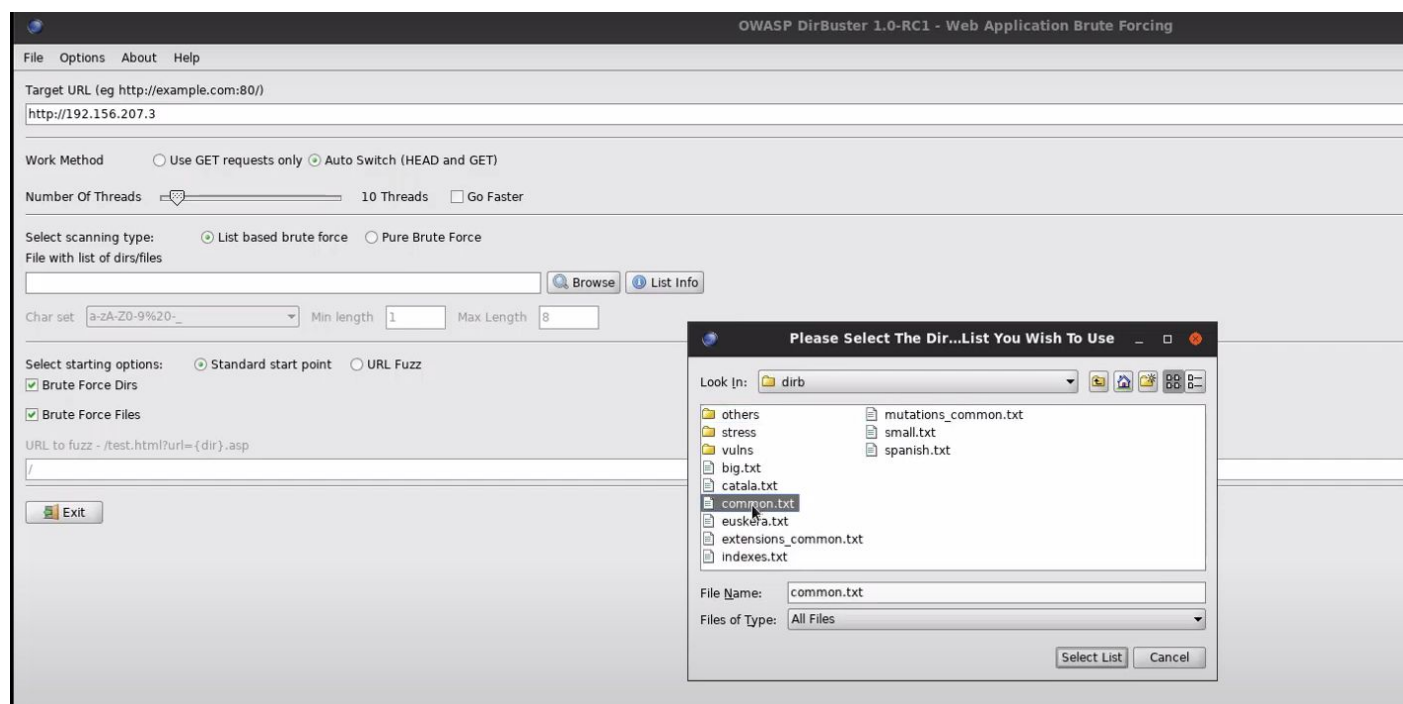
Click on “Wordlists” directory.



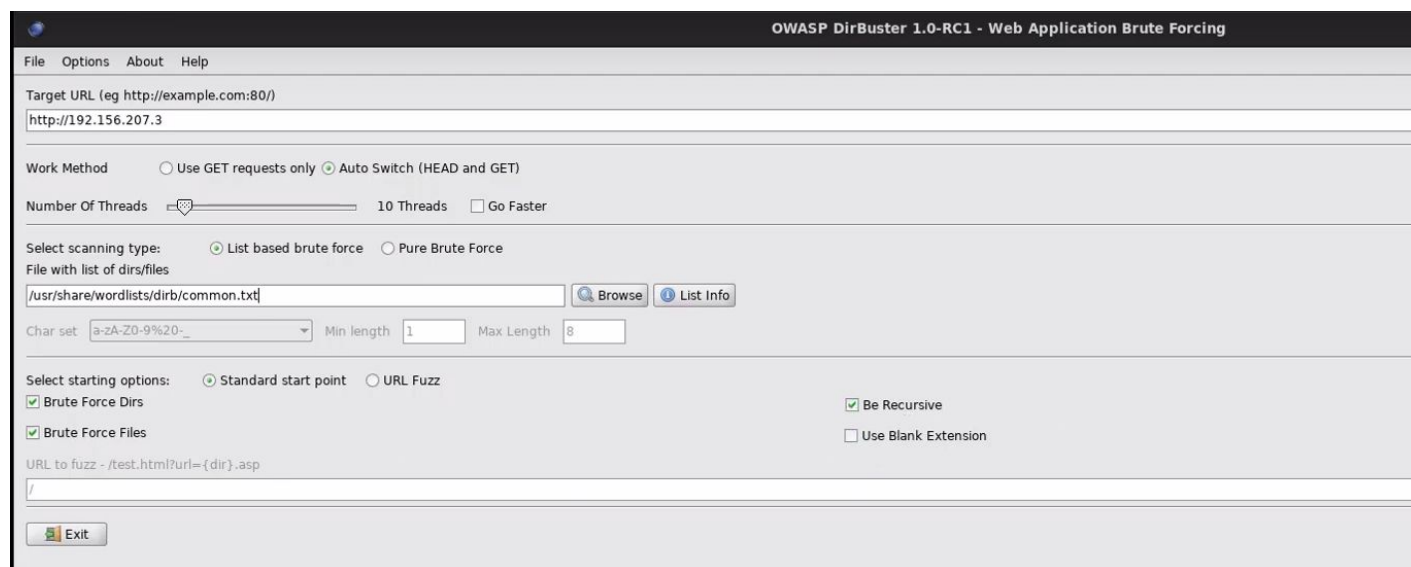
Choose “dirb” directory.



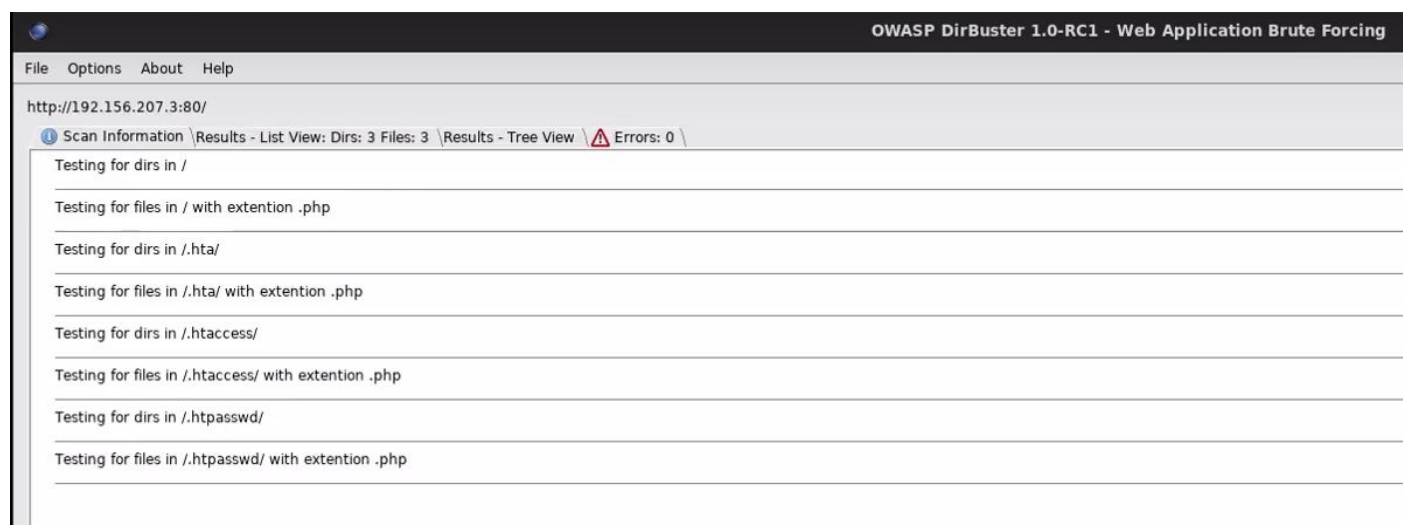
Select “common.txt” as the wordlist.



The wordlist is selected.



Step 6: Click on the Start button.



Wait for some time to get enough results.



Step 7: Click on the “Results - List Views” button in order to see the results.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://192.156.207.3:80/

Scan Information Results - List View: Dirs: 76 Files: 109 Results - Tree View Errors: 2

Type	Found	Response
Dir	/htaccess/	403
File	/hta.php	403
File	/htaccess.php	403
File	/htpasswd.php	403
File	/index.php	200
File	/set-up-database.php	200
Dir	/webservices/	200
Dir	/webservices/soap/	200
Dir	/ajax/	200
File	/webservices/soap/ws-user-account.php	200
File	/webservices/hta.php	403
Dir	/webservices/hta/	403
Dir	/webservices/htaccess/	403
File	/webservices/htaccess.php	403
File	/webservices/htpasswd.php	403
Dir	/webservices/htpasswd/	403
Dir	/webservices/rest/	200
File	/webservices/rest/hta.php	403
Dir	/webservices/soap/htaccess/	403
Dir	/webservices/soap/hta/	403
Dir	/ajax/hta/	403
File	/webservices/rest/ws-user-account.php	200
File	/webservices/soap/htaccess.php	403
Dir	/ajax/htaccess/	403
File	/webservices/soap/htpasswd.php	403
Dir	/ajax/htpasswd/	403
File	/ajax/hta.php	403
File	/webservices/soap/ws-lookup-dns-record.php	200
Dir	/webservices/soap/htpasswd/	403
File	/ajax/htaccess.php	403
File	/framer.html	200
File	/ajax/htpasswd.php	403
File	/webservices/rest/hta.php	403
File	/webservices/soap/ws-hello-world.php	200
Dir	/webservices/rest/hta/	403
File	/webservices/rest/htaccess.php	403
Dir	/webservices/rest/htaccess/	403
Dir	/webservices/test/	200
File	/webservices/rest/htpasswd.php	403

Current speed: 415 requests/sec
Average speed: (T) 362, (C) 417 requests/sec

Click on the “Results - Tree View” to get the results in tree format.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://192.156.207.3:80/

Scan Information Results - List View: Dirs: 79 Files: 119 Results - Tree View Errors: 2

Directory Structure	Response Code
54008	
403	460
403	455
403	460
403	458
403	463
403	463
200	239
200	5393
200	1510
200	1152
200	1723
200	2815
403	456
200	4710
200	177
200	2174
200	880

Step 8: Increase the threads up to 30 to get results faster. Enter 30 in the “Current number of threads”.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://192.156.207.3:80/

Scan Information Results - List View: Dirs: 79 Files: 119 Results - Tree View Errors: 2

Directory Structure	Response Code
. <td>200</td>	200
.hta	403
.htaccess	403
.hta.php	403
.htaccess.php	403
.htpasswd.php	403
index.php	200
set-up-database.php	200
webservices	200
soap	200
ws-user-account.php	200
.hta.php	403
.htaccess	403
.hta	403
.htaccess.php	403
.htpasswd.php	403
ws-lookup-dns-record.php	200
.htpasswd	403
ws-hello-world.php	200
lib	200
.hta.php	403
.hta	403
.htaccess	403
.htaccess.php	403
.htpasswd.php	403
.htpasswd	403
rest	200
test	200
ajax	200
framer.html	200
documentation	200
mutillidae-installation-on-xampp-win7.pdf	200
.hta.php	403

Current speed: 460 requests/sec
Average speed: (T) 418, (C) 464 requests/sec
Parse Queue Size: 0
Total Requests: 44379/738525
Current number of running threads: 10
30 Change
Time To Finish: 00:24:56

Click on the Change button.

OWASIDirBuster 1.0.0 - Web Application Brute Forcing

File Options About Help

http://192.156.207.3:80/

Scan Information \Results - List View: Dirs: 79 Files: 119 \Results - Tree View \Errors: 2 \

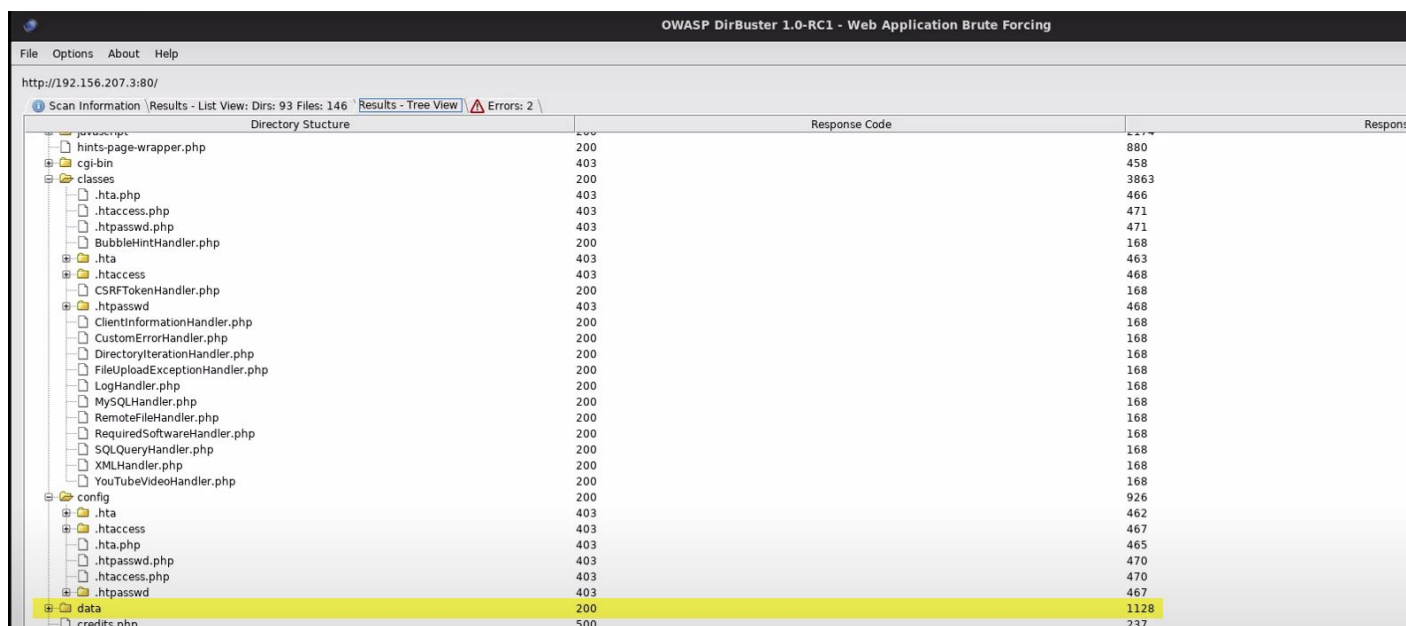
Directory Structure	Response Code	
..	200	54008
..	403	460
..	403	455
..	403	460
..	403	458
..	403	463
..	403	463
..	200	239
..	200	5393
..	200	1510
..	200	1816
..	200	337
..	403	475
..	403	477
..	403	472
..	403	480
..	403	480
..	200	6228
..	403	477
..	200	6079
..	200	3808
..	403	470
..	403	467
..	403	472
..	403	475
..	403	475
..	403	472
..	200	1178
..	200	1161
..	200	1152
..	200	1723
..	200	2815
..	200	1619416
..	403	472

Current speed: 908 requests/sec
Average speed: (T) 423, (C) 508 requests/sec
Parse Queue Size: 0
Total Requests: 45749/738525
Current number of running threads: 30

The threads are modified from 10 to 30.

Step 9: Find the data directory in the Results - Tree View.

Note: If the data directory is not available, Wait for a while or increase the number of threads.



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

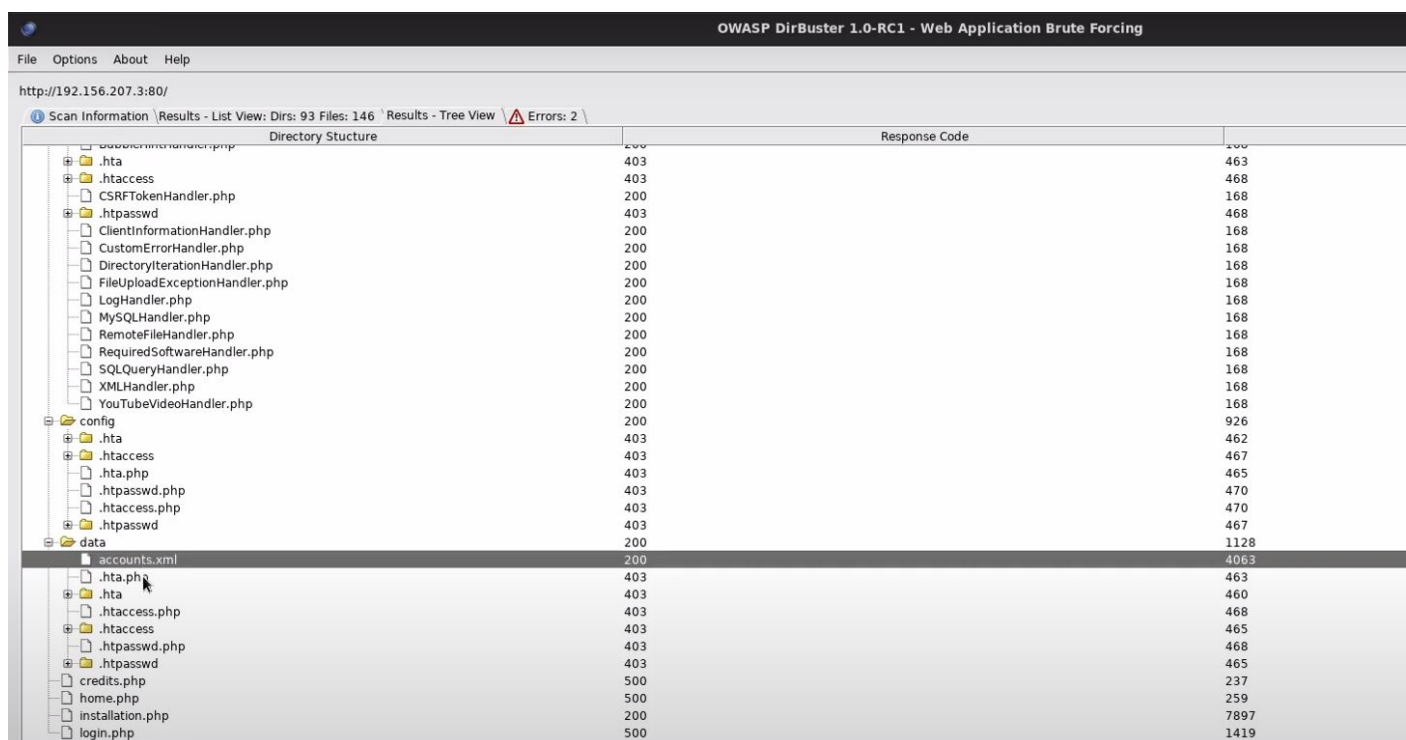
File Options About Help

http://192.156.207.3:80/

Scan Information Results - List View: Dirs: 93 Files: 146 Results - Tree View Errors: 2

Directory Structure	Response Code	Response
hints-page-wrapper.php	200	880
cgi-bin	403	458
classes	200	3863
.hta.php	403	466
.htaccess.php	403	471
.htpasswd.php	403	471
BubbleHintHandler.php	200	168
.hta	403	463
.htaccess	403	468
CSRFTokenHandler.php	200	168
.htpasswd	403	468
ClientInformationHandler.php	200	168
CustomErrorHandler.php	200	168
DirectoryIterationHandler.php	200	168
FileUploadExceptionHandler.php	200	168
LogHandler.php	200	168
MySQLHandler.php	200	168
RemoteFileHandler.php	200	168
RequiredSoftwareHandler.php	200	168
SQLQueryHandler.php	200	168
XMLHandler.php	200	168
YouTubeVideoHandler.php	200	168
config	200	926
.hta	403	462
.htaccess	403	467
.hta.php	403	465
.htpasswd.php	403	470
.htaccess.php	403	470
.htpasswd	403	467
data	200	1128
credits.php	500	237

Step 10: Click on the dropdown button to get the contents inside the data directory.




OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://192.156.207.3:80/

Scan Information Results - List View: Dirs: 93 Files: 146 Results - Tree View Errors: 2

Directory Structure	Response Code	Response
CustomErrorHandler.php	200	168
.hta	403	463
.htaccess	403	468
CSRFTokenHandler.php	200	168
.htpasswd	403	468
ClientInformationHandler.php	200	168
CustomErrorHandler.php	200	168
DirectoryIterationHandler.php	200	168
FileUploadExceptionHandler.php	200	168
LogHandler.php	200	168
MySQLHandler.php	200	168
RemoteFileHandler.php	200	168
RequiredSoftwareHandler.php	200	168
SQLQueryHandler.php	200	168
XMLHandler.php	200	168
YouTubeVideoHandler.php	200	168
config	200	926
.hta	403	462
.htaccess	403	467
.hta.php	403	465
.htpasswd.php	403	470
.htaccess.php	403	470
.htpasswd	403	467
data	200	1128
accounts.xml	200	4063
.hta.php	403	463
.hta	403	460
.htaccess.php	403	468
.htaccess	403	465
.htpasswd.php	403	468
.htpasswd	403	465
credits.php	500	237
home.php	500	259
installation.php	200	7897
login.php	500	1419



Account.xml is found inside the data directory.

References:

1. Dirbuster (<https://sourceforge.net/projects/dirbuster/>)
2. Mutillidae (<https://sourceforge.net/projects/mutillidae/>)