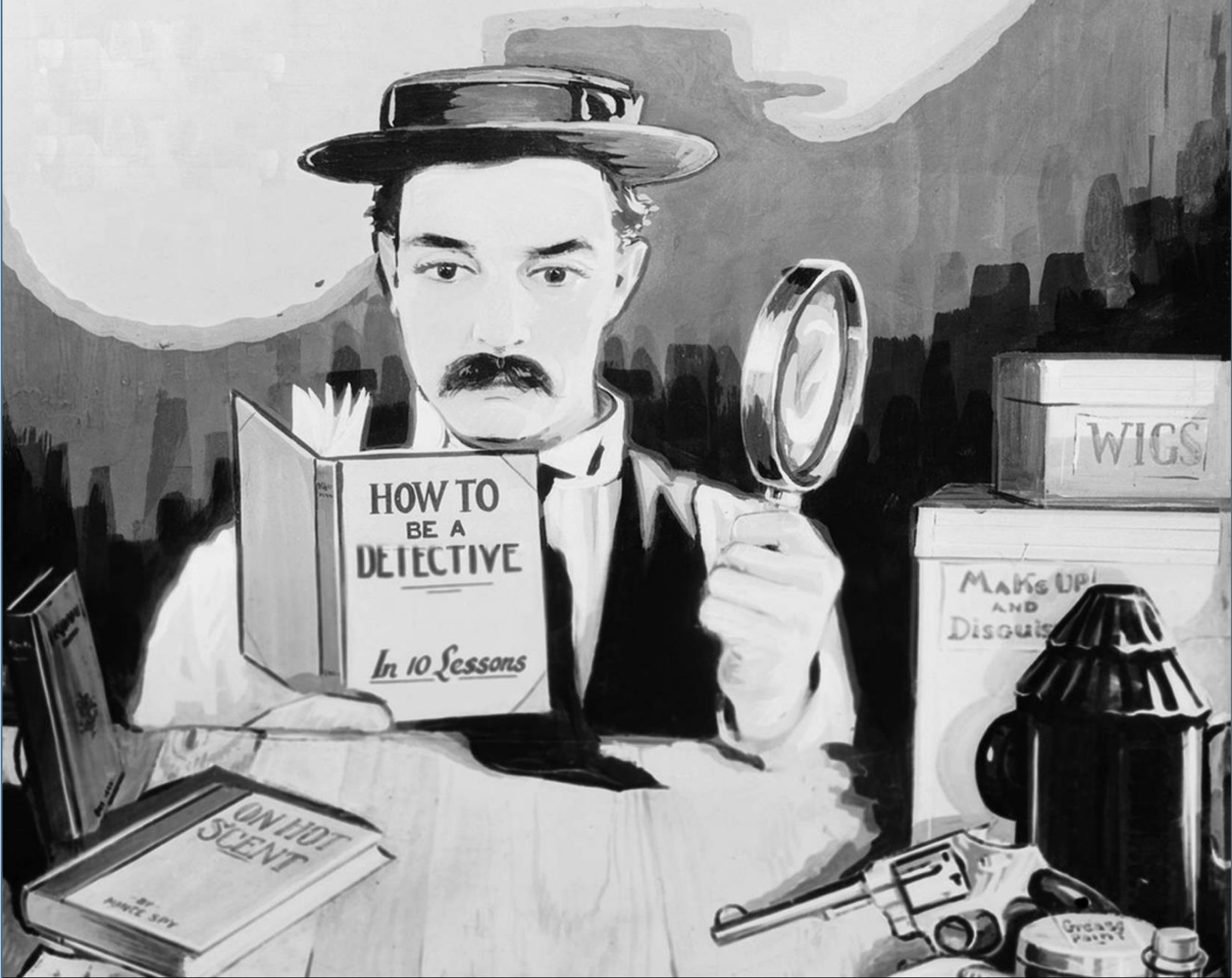


# A DETAILED GUIDE ON DIRBUSTER



**Contents**

- Introduction ..... 3**
- What is DirBuster? ..... 3**
- Default Mode ..... 3**
- Get Request Method ..... 4**
- Pure Brute Force (Numeric) ..... 6**
- Single Sweep (Non-recursive) ..... 8**
- Targeted Start..... 10**
- Blank Extensions ..... 11**
- Search by File Type (.txt) ..... 12**
- Changing the DIR List ..... 14**
- Following Redirects ..... 15**
- Attack through Proxy ..... 17**
- Adding File Extensions ..... 20**
- Evading Detective Measures ..... 24**

## Introduction

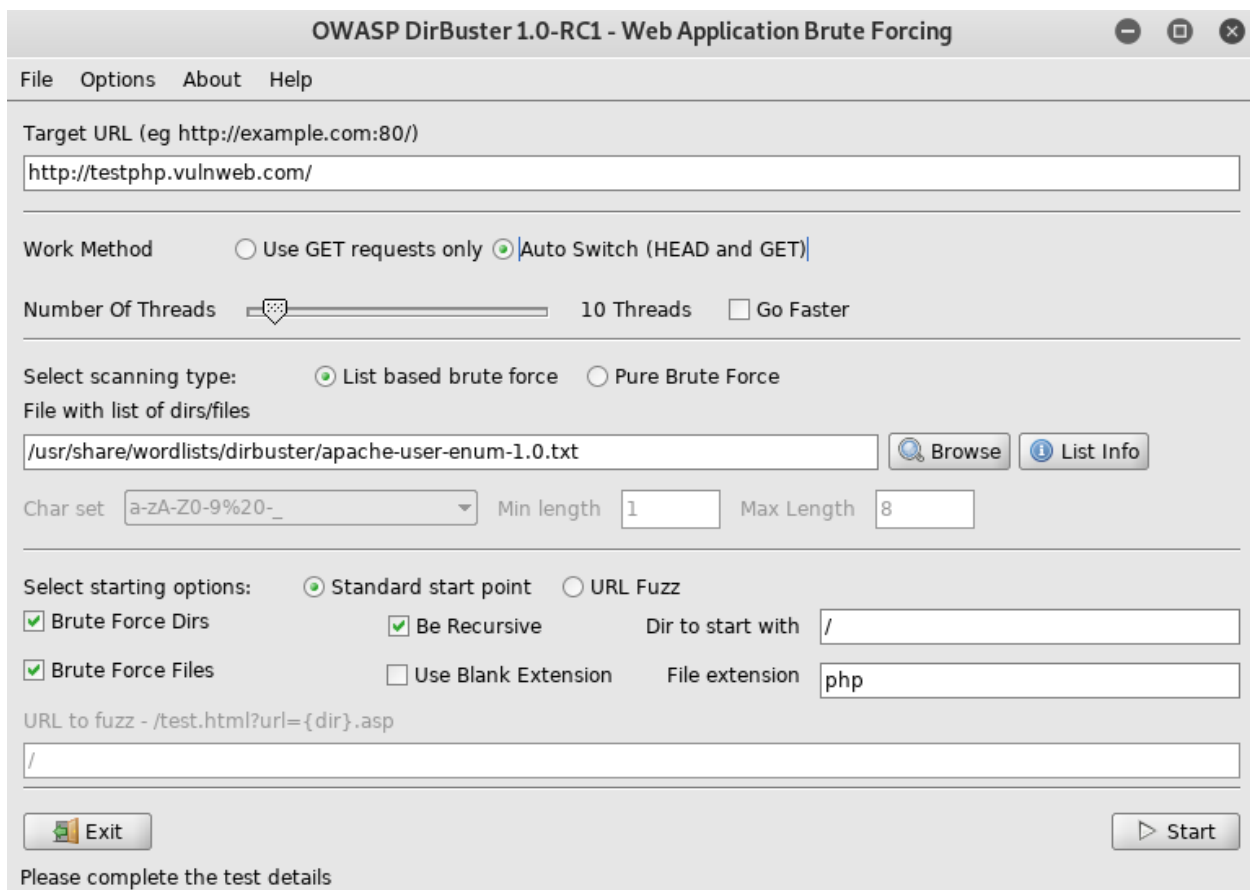
we are focusing on the transient directory using Kali Linux tool Dirbuster and trying to find hidden files and directories within a web server.

## What is DirBuster?

DirBuster is an application within the Kali arsenal that is designed to brute force web and application servers. The tool can brute force directories and files. The application lets users take advantage of multi-thread functionality to get things moving faster. In this article, we will give you an overview of the tool and its basic functions.

## Default Mode

We start DirBuster and only input `http://testphp.vulnweb.com/` in the target URL field. Leave the rest of the options as they are. DirBuster will now auto switch between HEAD and GET requests to perform a list based brute force attack.



The screenshot shows the OWASP DirBuster 1.0-RC1 application window titled "OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing". The interface includes a menu bar with "File", "Options", "About", and "Help". The main configuration area is as follows:

- Target URL (eg http://example.com:80/):** `http://testphp.vulnweb.com/`
- Work Method:**  Use GET requests only,  Auto Switch (HEAD and GET)
- Number Of Threads:** A slider set to 10 Threads, with a  Go Faster checkbox.
- Select scanning type:**  List based brute force,  Pure Brute Force
- File with list of dirs/files:** `/usr/share/wordlists/dirbuster/apache-user-enum-1.0.txt`, with  and  buttons.
- 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:** `/`
- and  buttons.

At the bottom, a message reads: "Please complete the test details".

Let's hit Start. DirBuster gets to work and starts brute forcing and we see various files and directories popping up in the result window.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://testphp.vulnweb.com:80/

Scan Information Results - List View: Dirs: 5 Files: 11 Results - Tree View Errors: 0

Type	Found	Response	Size
Dir	/	200	4290
File	/index.php	200	196
File	/categories.php	200	196
File	/artists.php	200	196
File	/disclaimer.php	200	196
File	/cart.php	200	196
File	/guestbook.php	200	196
Dir	/AJAX/	200	196
File	/AJAX/index.php	200	196
File	/login.php	200	196
File	/userinfo.php	302	220
Dir	/Mod_Rewrite_Shop/	200	196
Dir	/hpp/	200	196
Dir	/images/	200	154

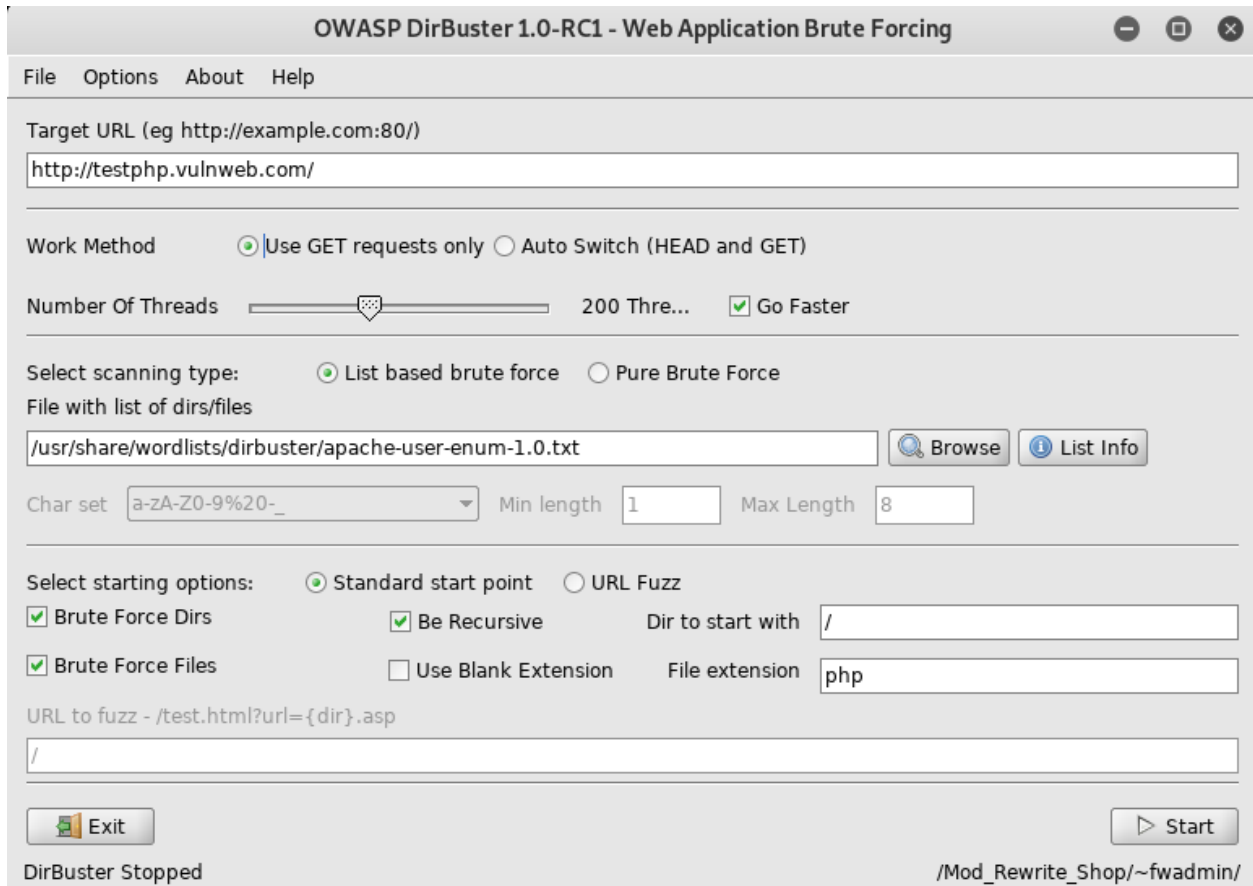
Current speed: 55 requests/sec (Select and right click for more options)  
 Average speed: (T) 50, (C) 53 requests/sec  
 Parse Queue Size: 0  
 Total Requests: 701/107037  
 Current number of running threads: 10  
 Time To Finish: 00:33:26

Back Pause Stop Report

DirBuster Stopped /Mod\_Rewrite\_Shop/~fwadmin/

## Get Request Method

We will now set DirBuster to only use the GET request method. To make things go a little faster, the thread count is set to 200 and the "Go Faster" checkbox is checked.



In the Results – Tree View we can see findings.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

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

Scan Information Results - List View: Dirs: 6 Files: 15 Results - Tree View Errors: 0

Directory Structure	Response Code	Response Size
/	200	4290
index.php	200	4290
artists.php	200	4655
categories.php	200	5454
disclaimer.php	200	4861
cart.php	200	4234
guestbook.php	200	4725
AJAX	200	4430
login.php	200	4865
userinfo.php	302	234
Mod_Rewrite_Shop	200	1171
hpp	200	399

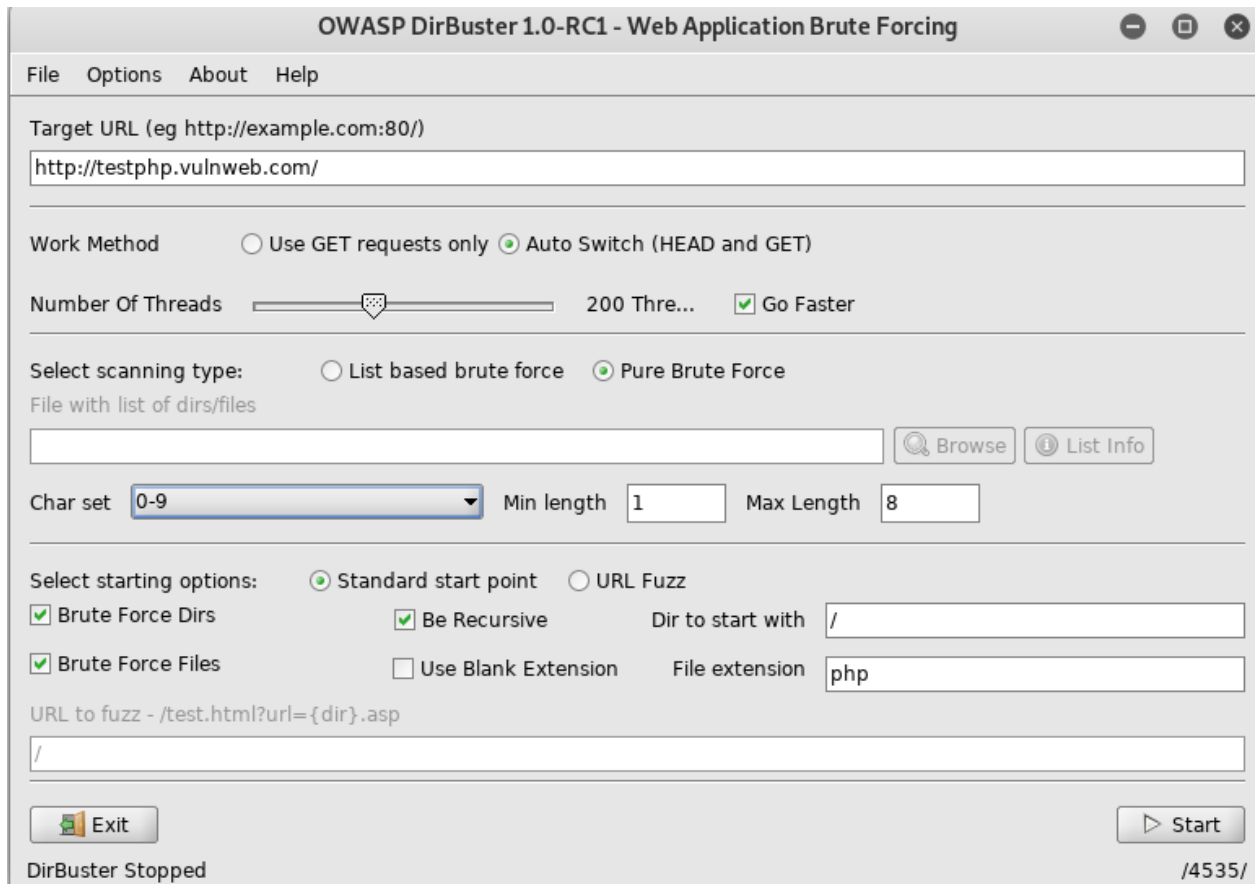
Current speed: 898 requests/sec (Select and right click for more options)  
 Average speed: (T) 856, (C) 943 requests/sec  
 Parse Queue Size: 14083  
 Total Requests: 19696/124890  
 Current number of running threads: 200  
 Time To Finish: 00:01:51

Exit Start

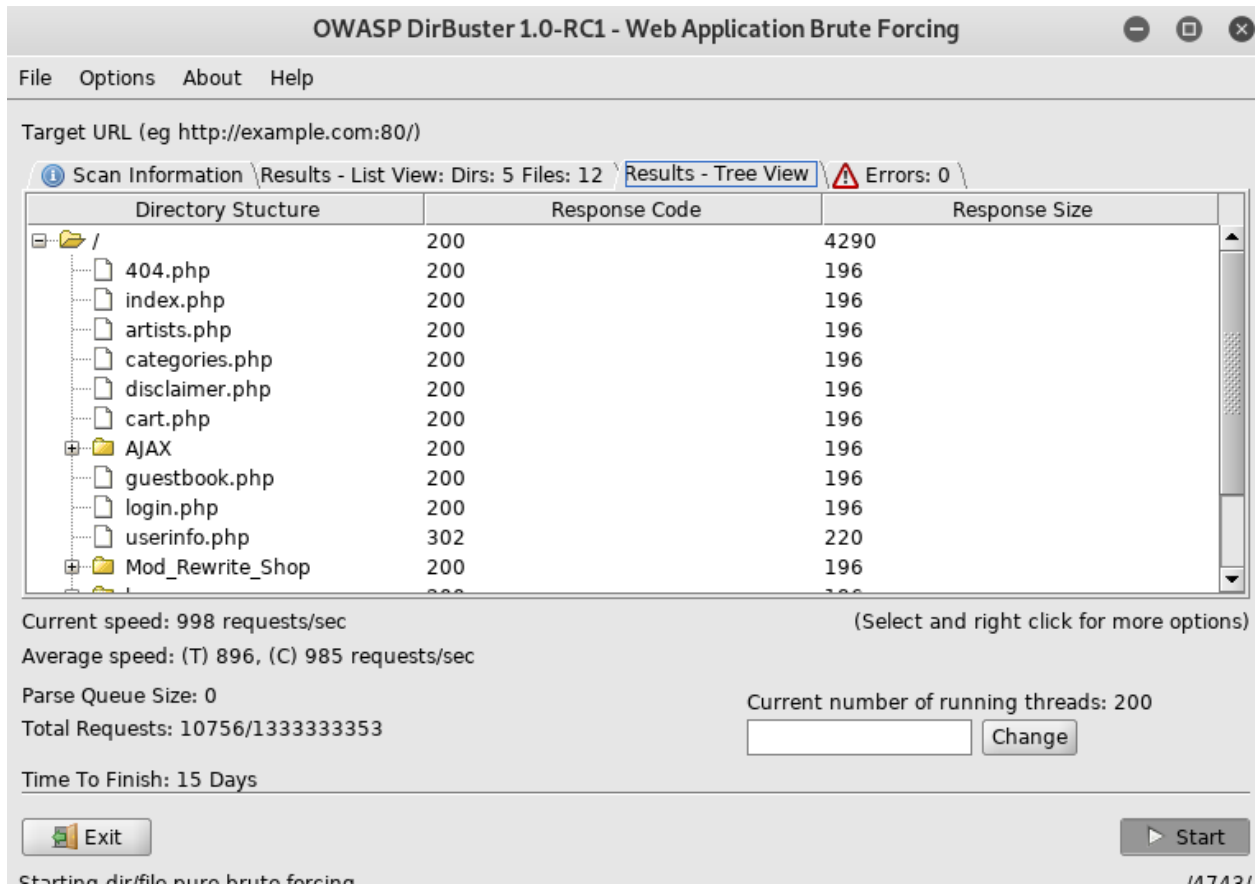
Starting dir/file list based brute forcing /Mod\_Rewrite\_Shop/images/~axe/

## Pure Brute Force (Numeric)

The way DirBuster performs this step allows a lot of control over the attack process. In this set we will be using only numerals to perform a pure brute force attack. This is done by selecting "Pure Brute Force" in the scanning type option and selecting "0-9" in the charset drop-down menu. By default, the minimum and maximum character limits are set.



In the Results – Tree View we can see findings.



## Single Sweep (Non-recursive)

We will now perform a single sweep brute force where the dictionary words are used only once. To achieve this, we will unselect the "Be Recursive" checkbox.



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

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

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

Number Of Threads  200 Thre...  Go Faster

Select scanning type:  List based brute force  Pure Brute Force

File with list of dirs/files

Char set  Min length  Max Length

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

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

Please complete the test details

In the Results – ListView we can see findings.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://testphp.vulnweb.com:80/

Scan Information Results - List View: Dirs: 0 Files: 11 Results - Tree View Errors: 0

Type	Found	Response	Size
Dir	/	200	4290
File	/index.php	200	196
File	/artists.php	200	196
File	/categories.php	200	196
File	/disclaimer.php	200	196
File	/cart.php	200	196
File	/guestbook.php	200	196
Dir	/AJAX/	200	196
File	/AJAX/index.php	200	196
File	/login.php	200	196
File	/userinfo.php	302	220
Dir	/Mod_Rewrite_Shop/	200	196
Dir	/hpp/	200	196
Dir	/images/	200	154

Current speed: 746 requests/sec (Select and right click for more options)

Average speed: (T) 825, (C) 897 requests/sec

Parse Queue Size: 0

Total Requests: 10734/17857

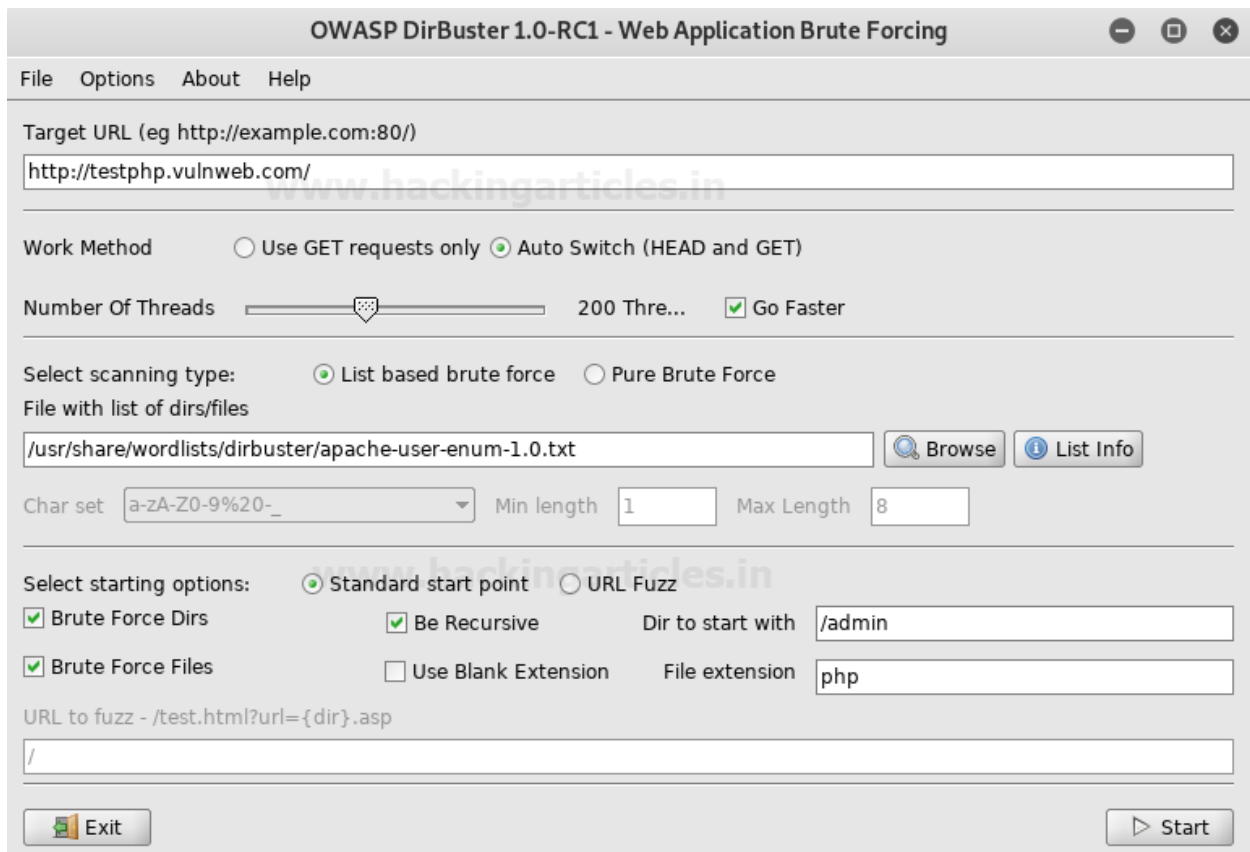
Current number of running threads: 200

Time To Finish: 00:00:07

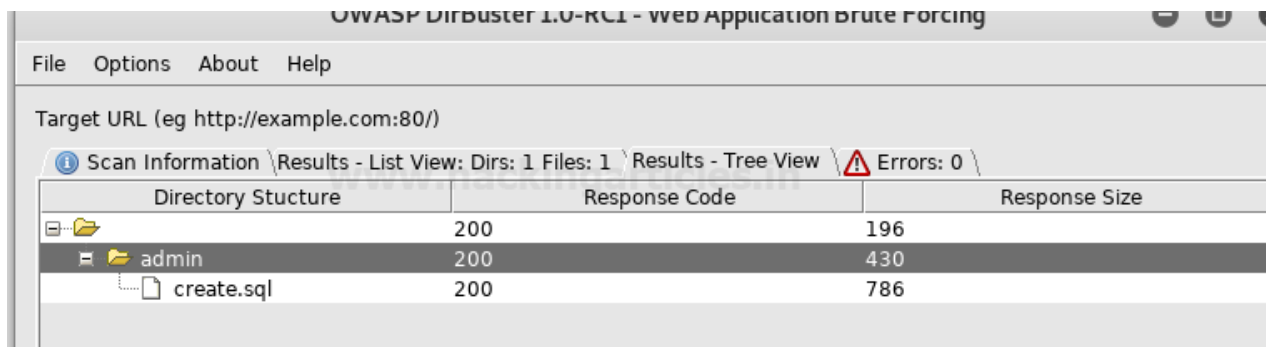
Back Pause Stop Report

## Targeted Start

Further exploring the control options provided by DirBuster, we will set it up to start looking at the "admin" directory. In the "Dir to start with" field, type "/admin" and hit start.

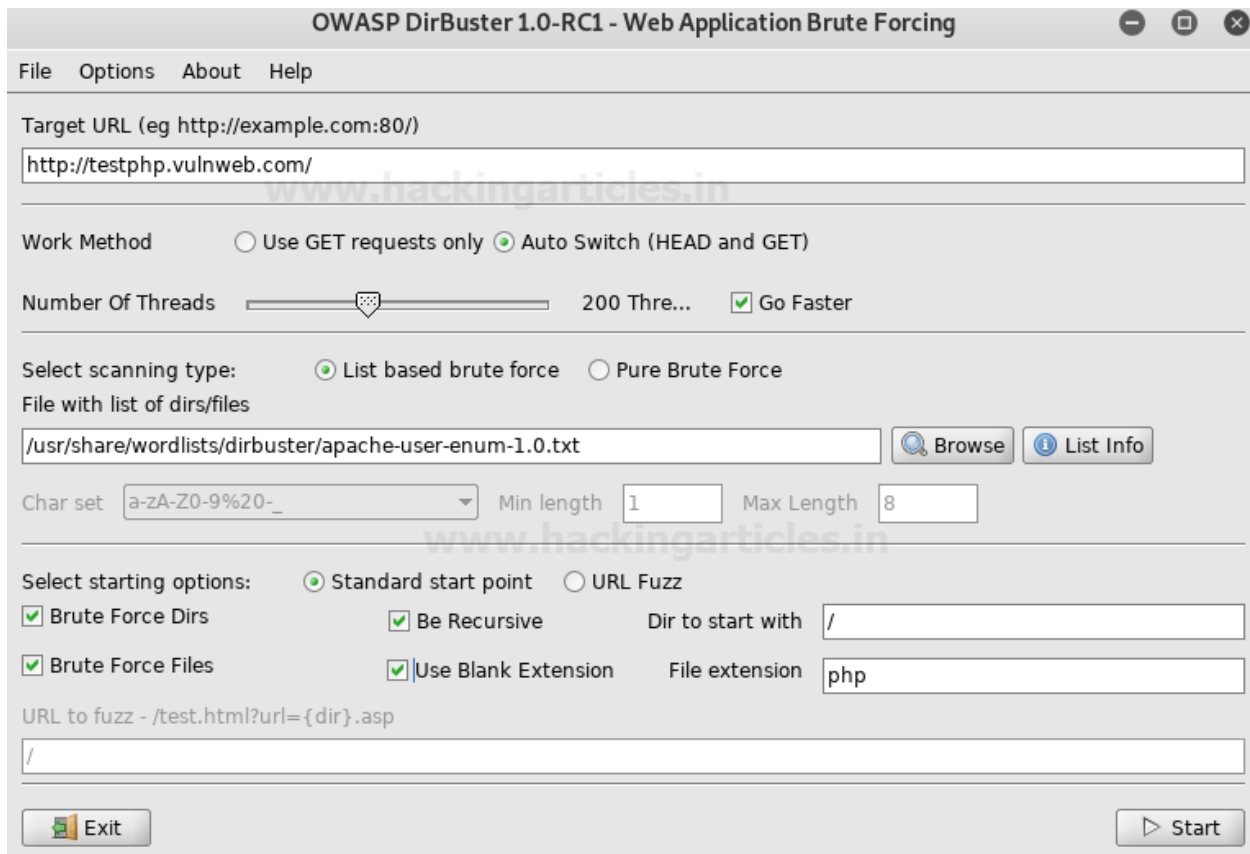


In the Results – Tree View we can see findings.

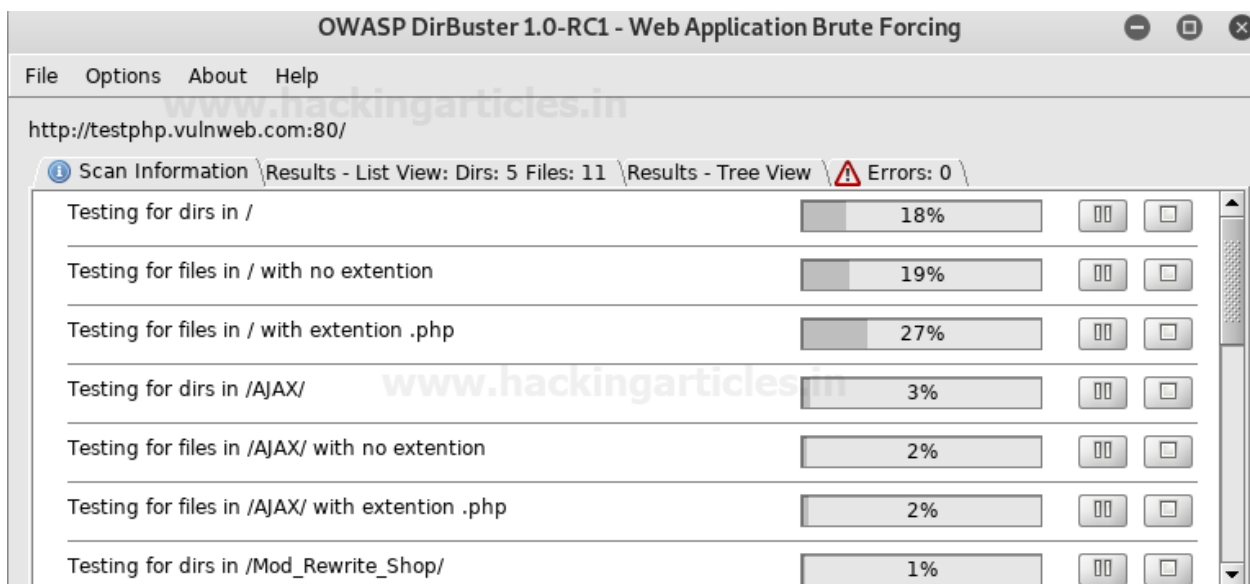


## Blank Extensions

DirBuster can also look into directories with a blank extension. This could potentially uncover data that might be otherwise left untouched. All we do is check the "Use Blank Extension" checkbox.

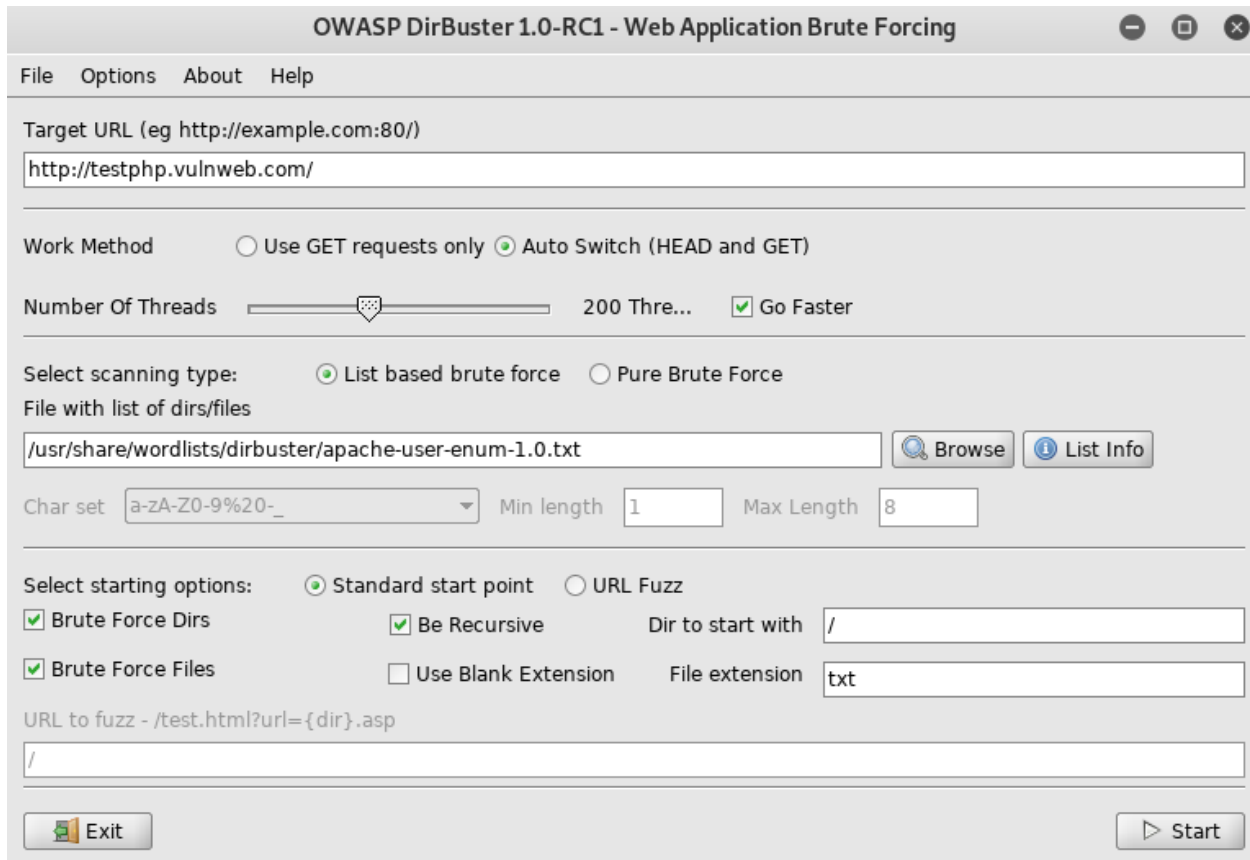


We can see the processing happen and DirBuster testing to find directories with blank extensions.

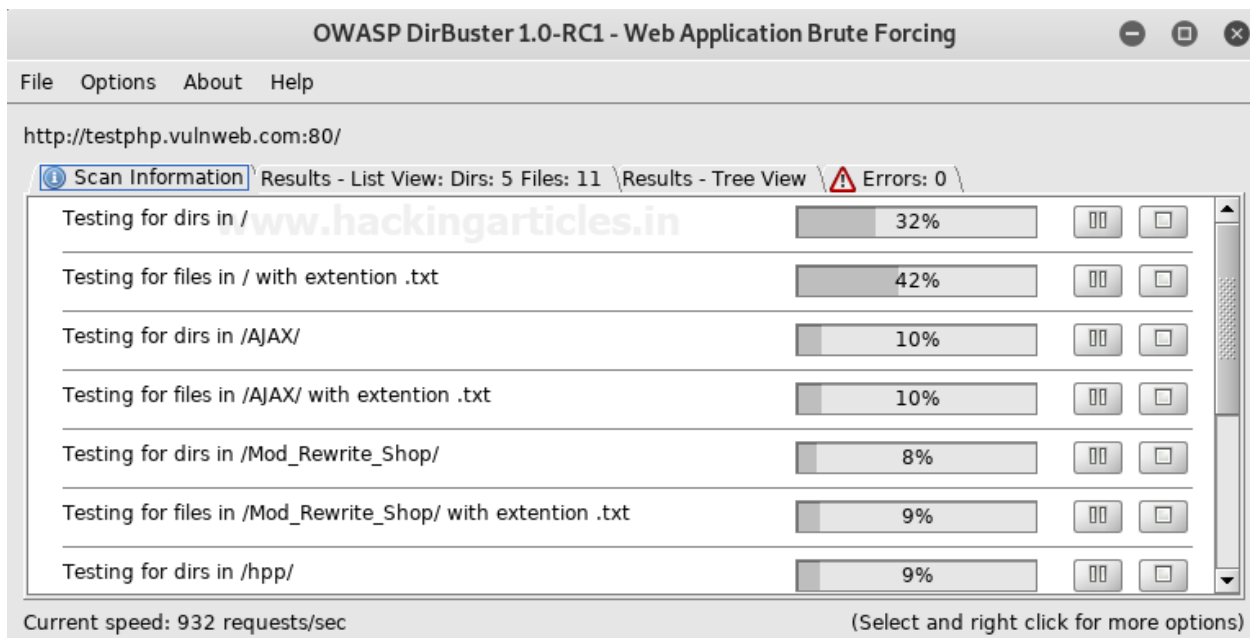


## Search by File Type (.txt)

We will be setting the file extension type to .txt, DirBuster will look specifically for files with a .txt extension. Type ".txt" in the File extension field and hit "Start."



We can see the processing happen and DirBuster testing to find directories with a .txt extension.

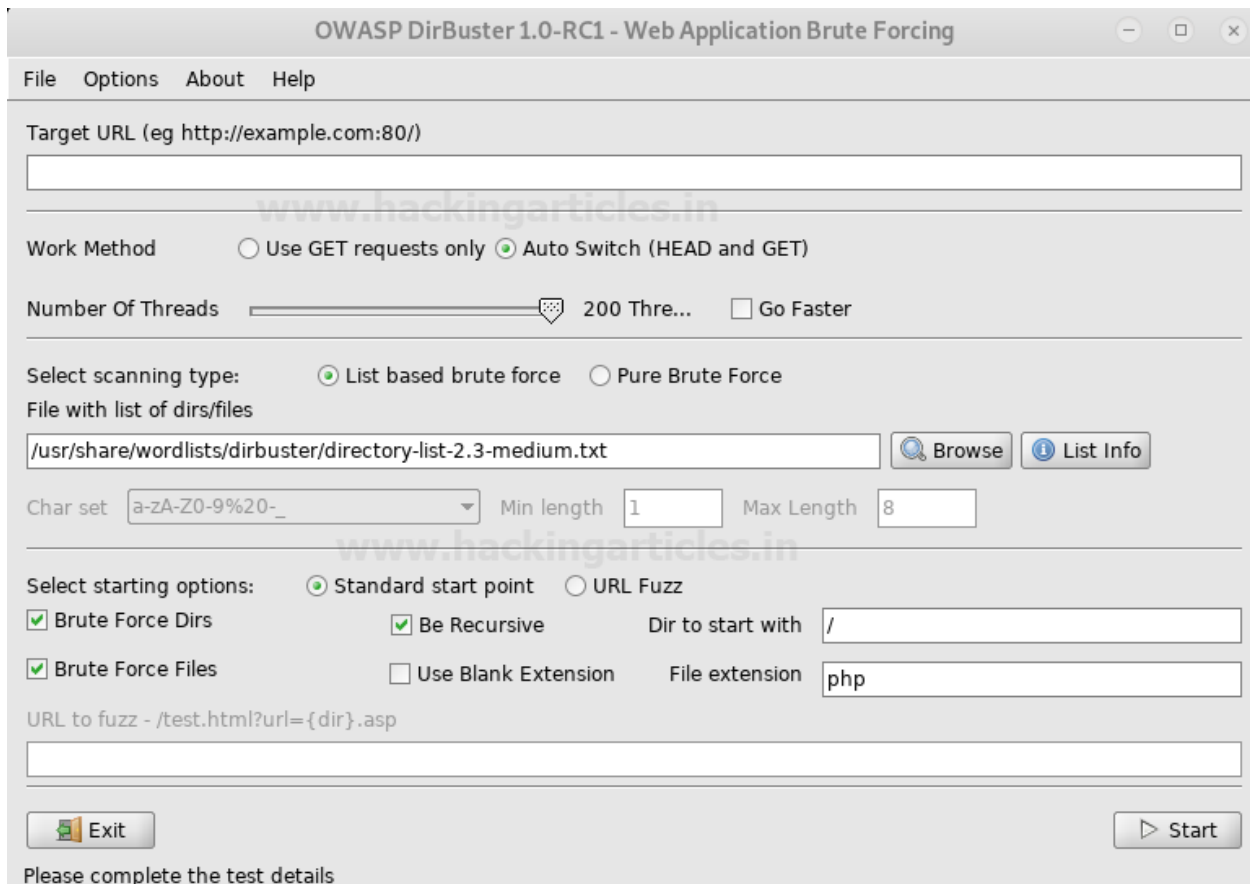


## Changing the DIR List

We will now be changing the directory list in DirBuster. Options > Advanced Options > DirBuster Options > Dir list to use. Here is where we can browse and change the list to “directory-list-2.3-medium.txt”, found at /usr/share/dirbuster/wordlists/ in Kali.

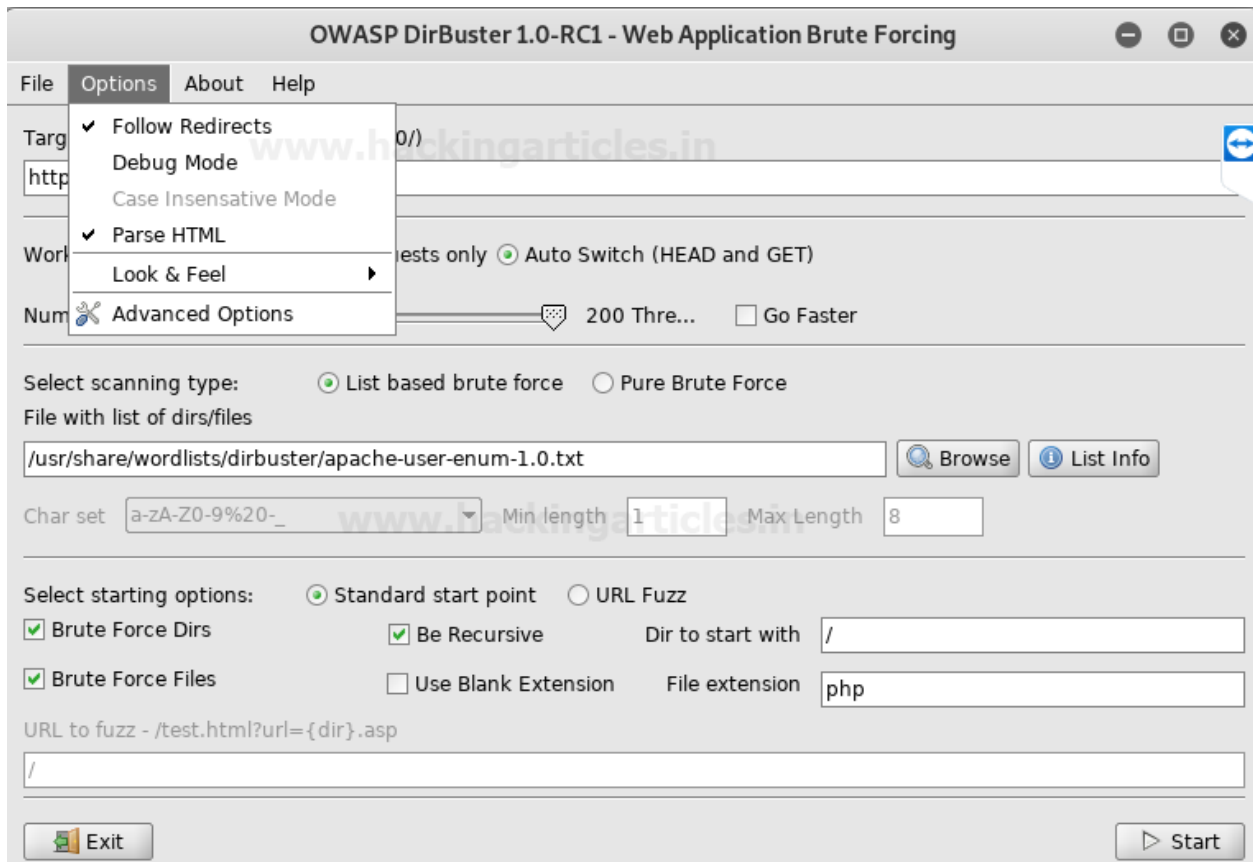


We can see the word list is now set.

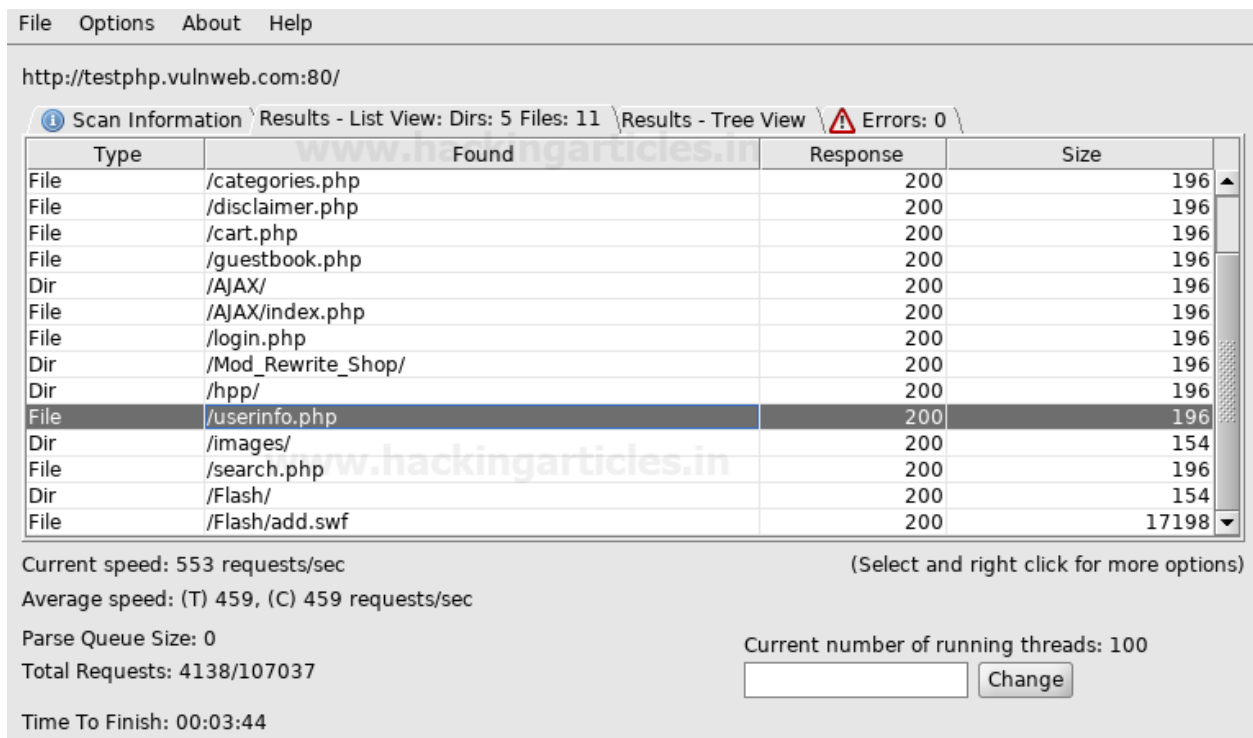


## Following Redirects

DirBuster by default is not set to follow redirects during the attack, but we can enable this option under Options > Follow Redirects.

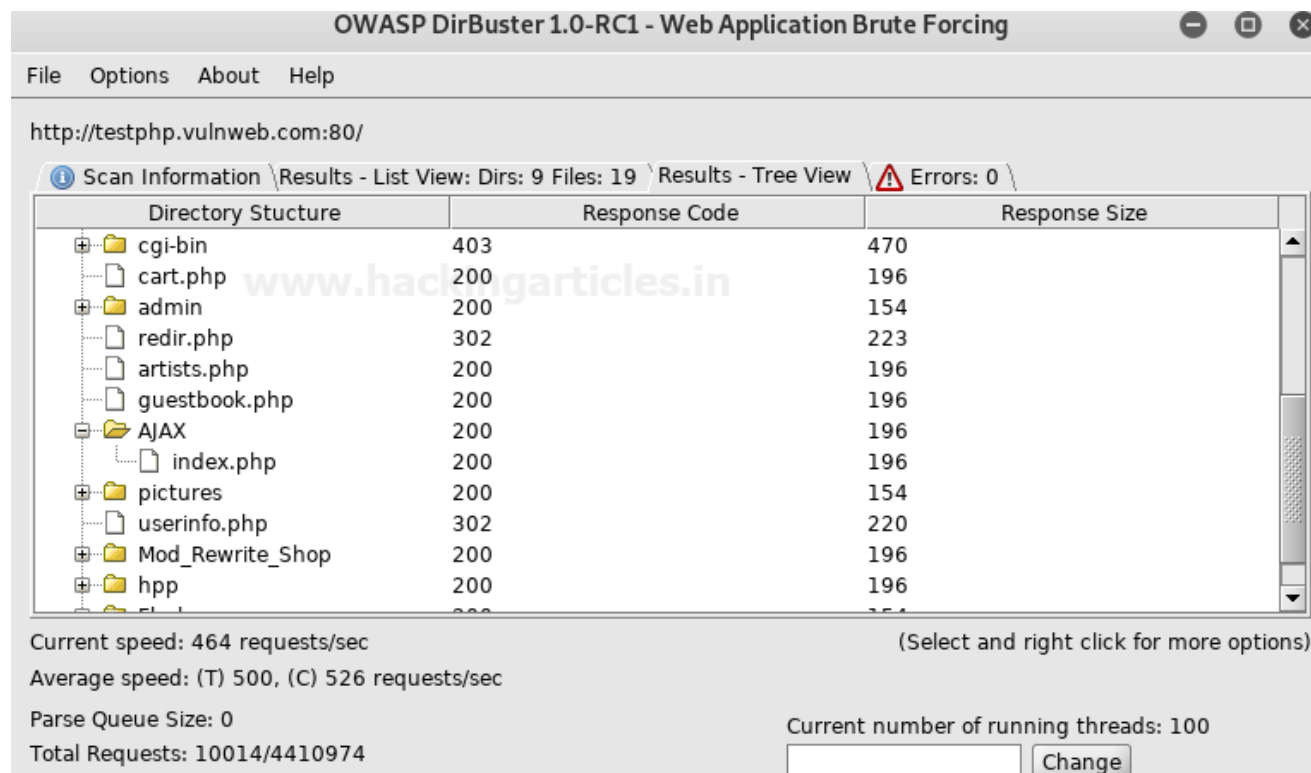


We can see the results in the scan information as the test progresses.





Results in the Tree View.



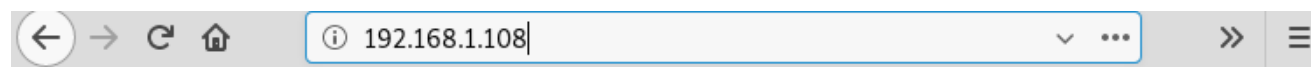
The screenshot shows the OWASP DirBuster 1.0-RC1 interface. The title bar reads "OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing". The address bar shows "http://testphp.vulnweb.com:80/". The main window displays a table of scan results in a tree view. The table has three columns: "Directory Structure", "Response Code", and "Response Size". The results are as follows:

Directory Structure	Response Code	Response Size
cg-bin	403	470
cart.php	200	196
admin	200	154
redir.php	302	223
artists.php	200	196
guestbook.php	200	196
AJAX	200	196
index.php	200	196
pictures	200	154
userinfo.php	302	220
Mod_Rewrite_Shop	200	196
hpp	200	196

Below the table, the interface shows performance metrics: "Current speed: 464 requests/sec", "Average speed: (T) 500, (C) 526 requests/sec", "Parse Queue Size: 0", and "Total Requests: 10014/4410974". A "Change" button is visible next to the "Current number of running threads: 100" indicator.

## Attack through Proxy

DirBuster can also attack using a proxy. In this scenario, we try to open a webpage at 192.168.1.108 but are denied access.



## Access forbidden!

You don't have permission to access the requested directory. There is either no index document or the directory is read-protected.

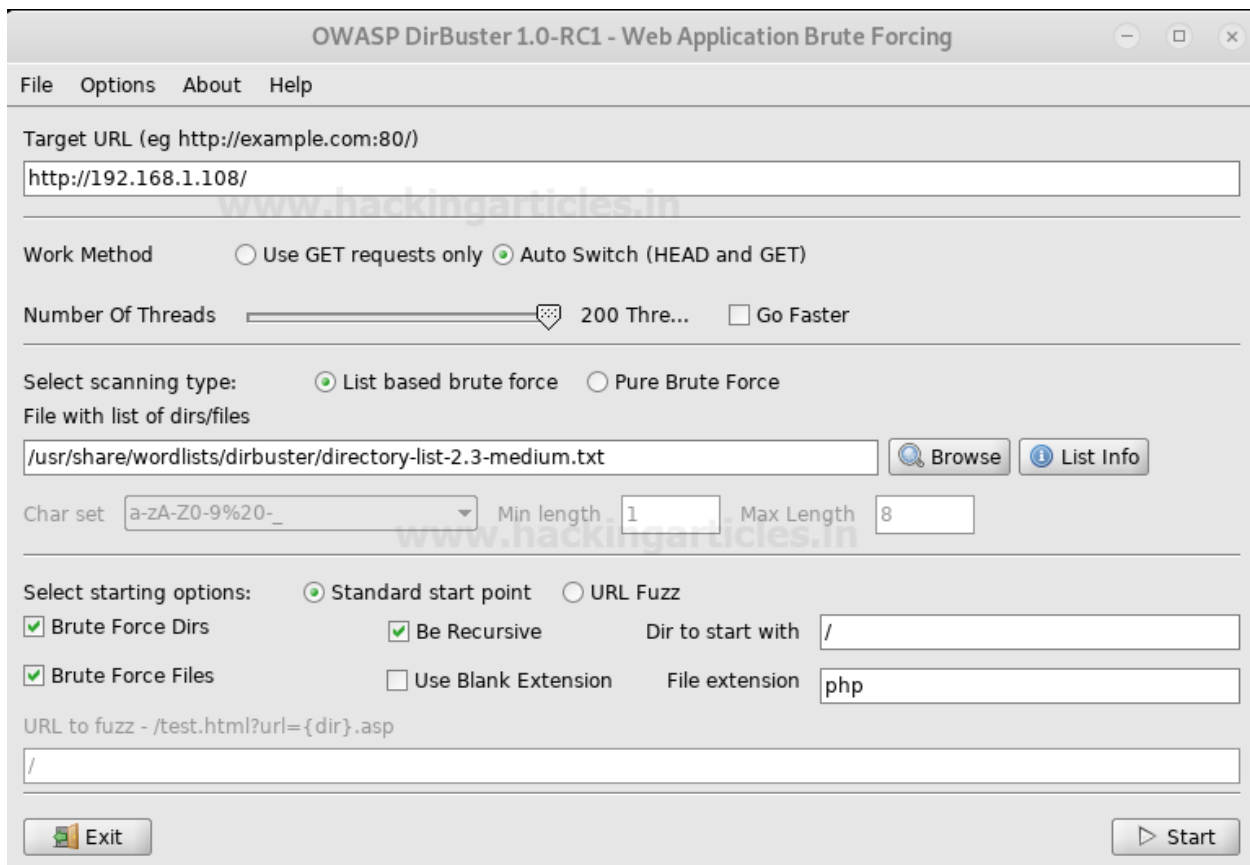
If you think this is a server error, please contact the [webmaster](#).

## Error 403

[192.168.1.108](http://192.168.1.108)

Apache

We set the IP in DirBuster as the attack target.



Before we start the attack, we set up the proxy option under Options > Advance Options > Http Options. Here we check the "Run through a proxy" checkbox, input the IP 192.168.1.108 in the Host field, and set the port to 3129

**DirBuster 1.0-RC1 - Advanced Options**

HTML Parsing Options \ Authentication Options \ **Http Options** \ Scan Options \ DirBuster Options

[www.hackingarticles.in](http://www.hackingarticles.in)

Custom HTTP Headers

Header	Value

Add New Custom HTTP Header

:

---

Http User Agent

[www.hackingarticles.in](http://www.hackingarticles.in)

Proxy Information & Authentication

Run Through a Proxy

Host  Port

Use Proxy Authentificati...

Realm  (Leave blank if not required)

User Name  Password

We can see the test showing results.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://192.168.1.108:80/

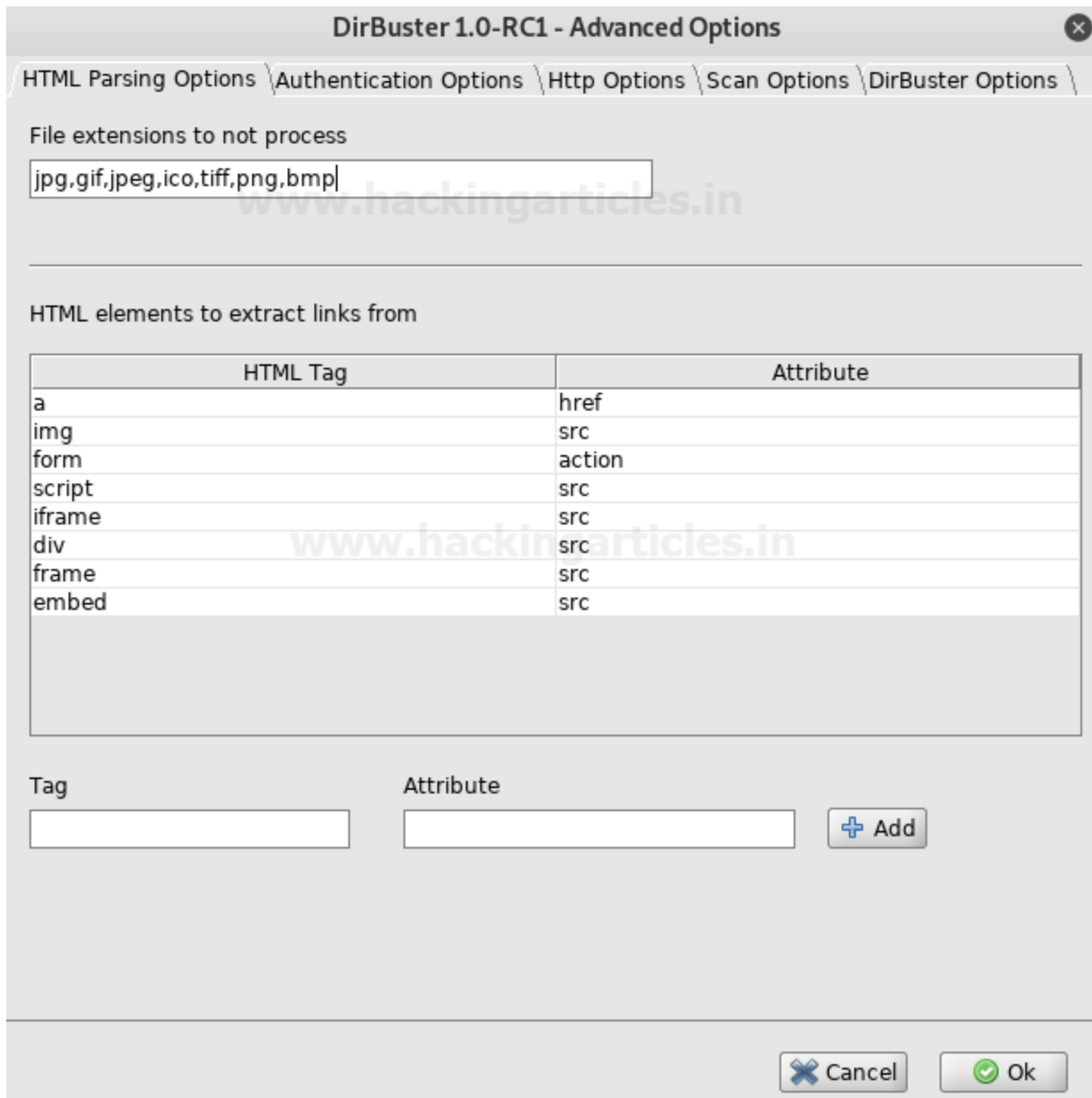
Scan Information Results - List View: Dirs: 12 Files: 4 Results - Tree View Errors: 0

Type	Found	Response	Size
Dir	/	200	3784
Dir	/error/	403	429
Dir	/icons/	200	344
Dir	/error/include/	403	429
Dir	/icons/small/	200	344
Dir	/blog/	200	410
Dir	/blog/wp-content/	200	331
File	/blog/wp-content/index.php	200	331
Dir	/blog/wp-content/themes/	200	331
Dir	/blog/wp-content/uploads/	403	429
File	/blog/wp-content/themes/index.php	200	331
Dir	/blog/wp-includes/	403	429
Dir	/blog/wp-includes/images/	403	429
Dir	/blog/wp-includes/images/media/	403	429

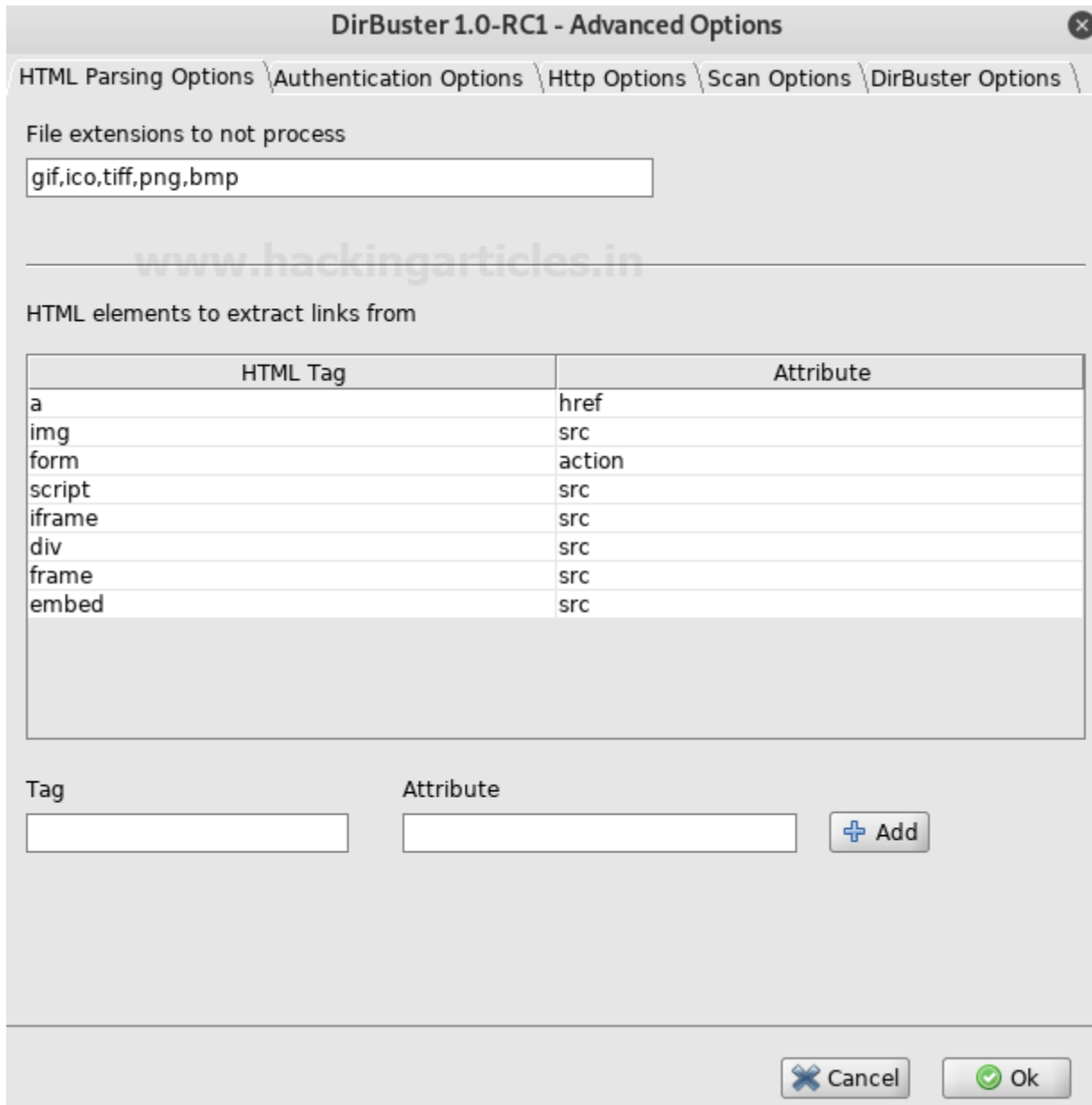
Current speed: 893 requests/sec (Select and right click for more options)  
Average speed: (T) 901, (C) 870 requests/sec

## Adding File Extensions

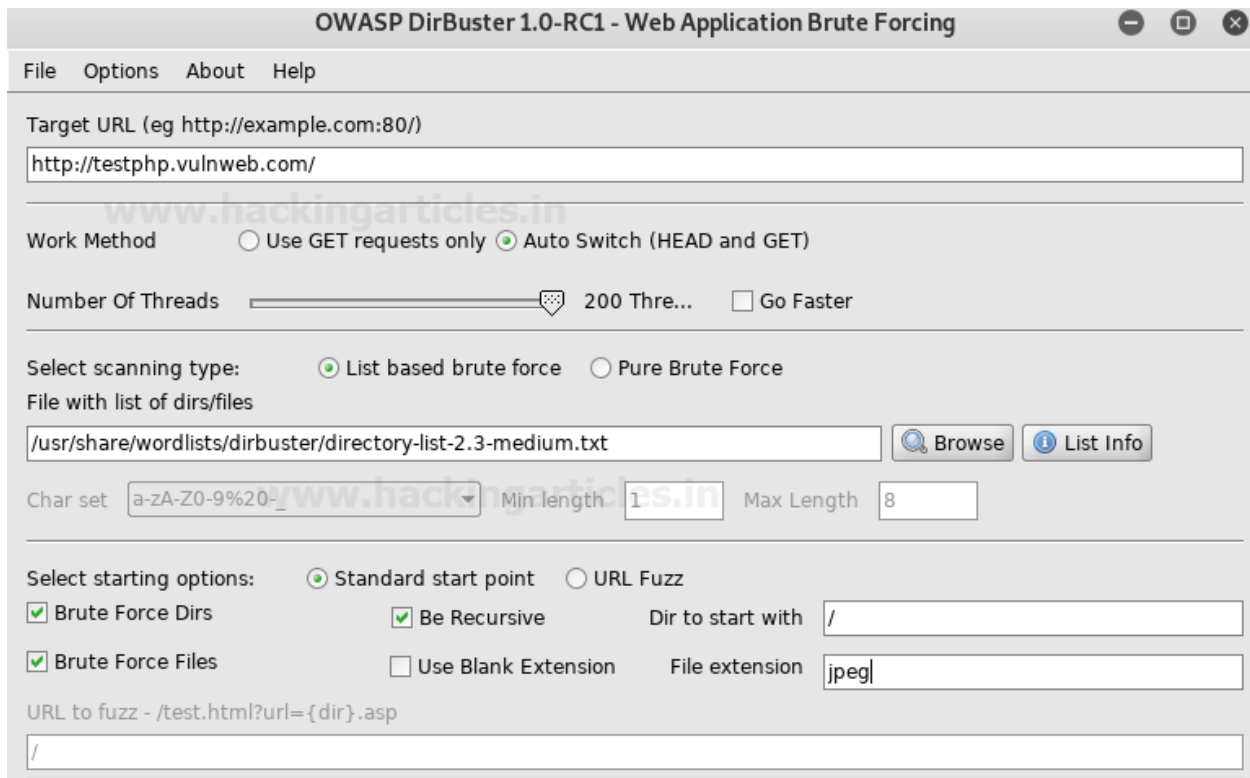
Some file extensions are not set to be searched for in DirBuster, mostly image formats. We can add these to be searched for by navigating to Options > Advanced Options > HTML Parsing Options.



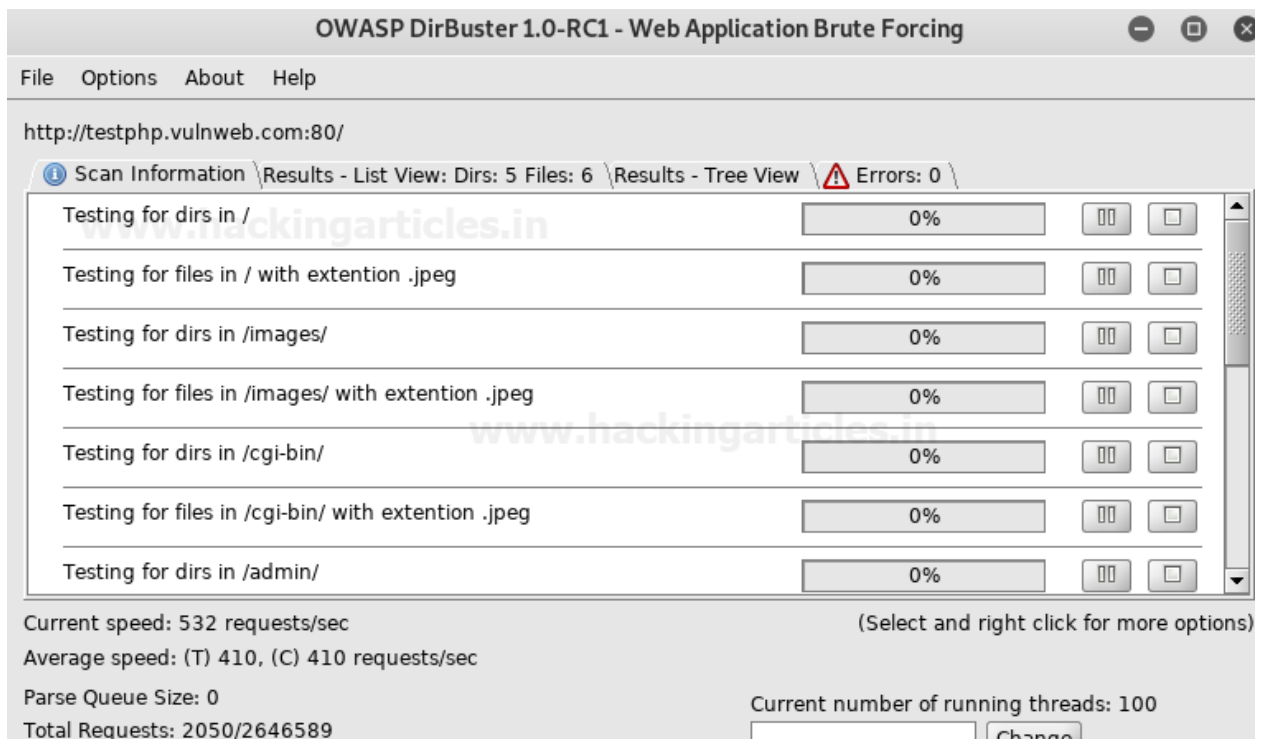
We will delete jpeg in this instance and click OK.



In the File Extension field we will type in "jpeg" to explicitly tell DirBuster to look for .jpeg format files.

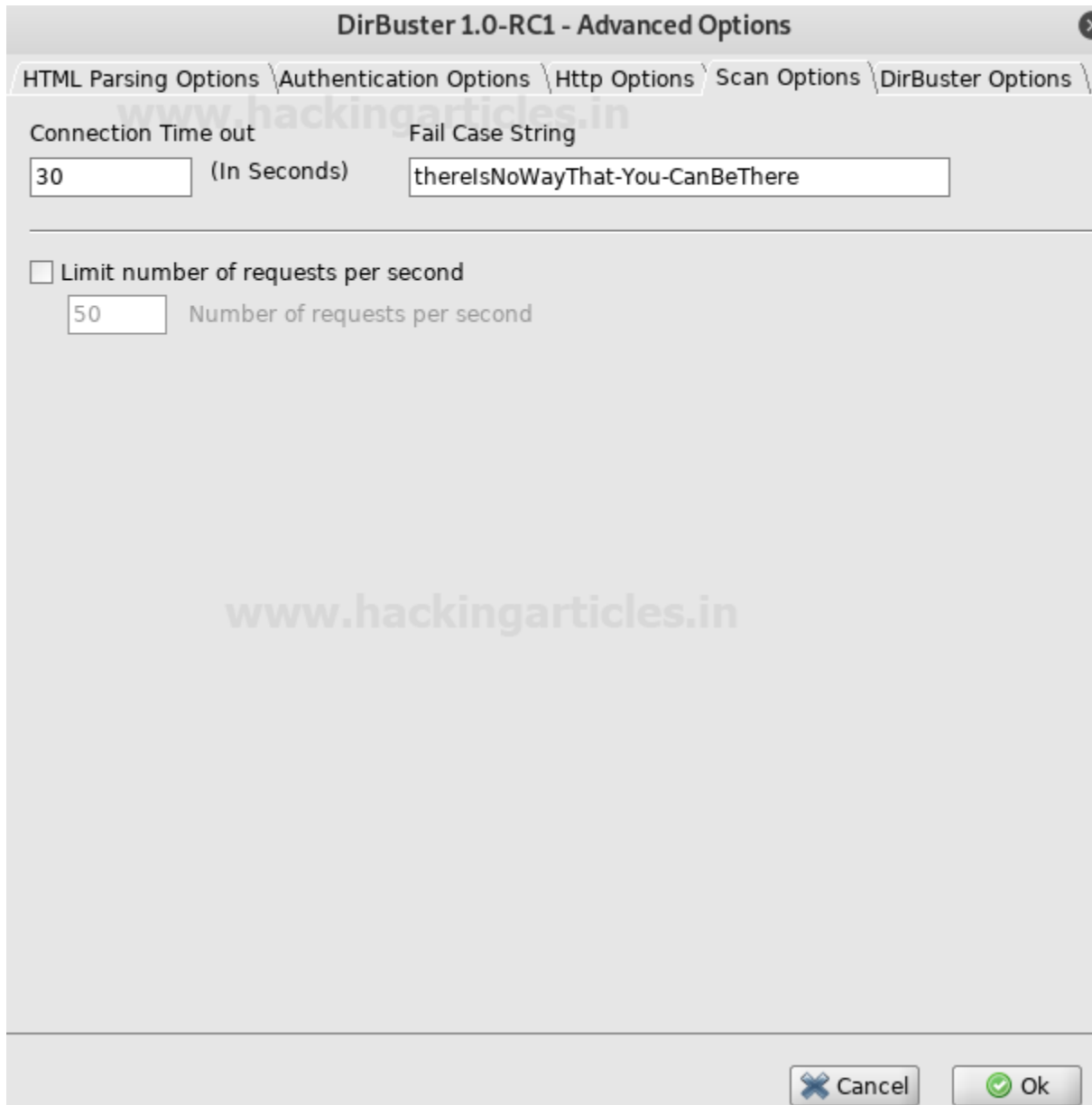


We can see in the testing process, DirBuster is looking for and finding jpeg files.



## Evading Detective Measures

Exceeding the warranted requests per second during an attack is a sure shot way to get flagged by any kind of detective measures put into place. DirBuster lets us control the requests per second to bypass this defense. Options > Advanced Options > Scan Options is where we can enable this setting.

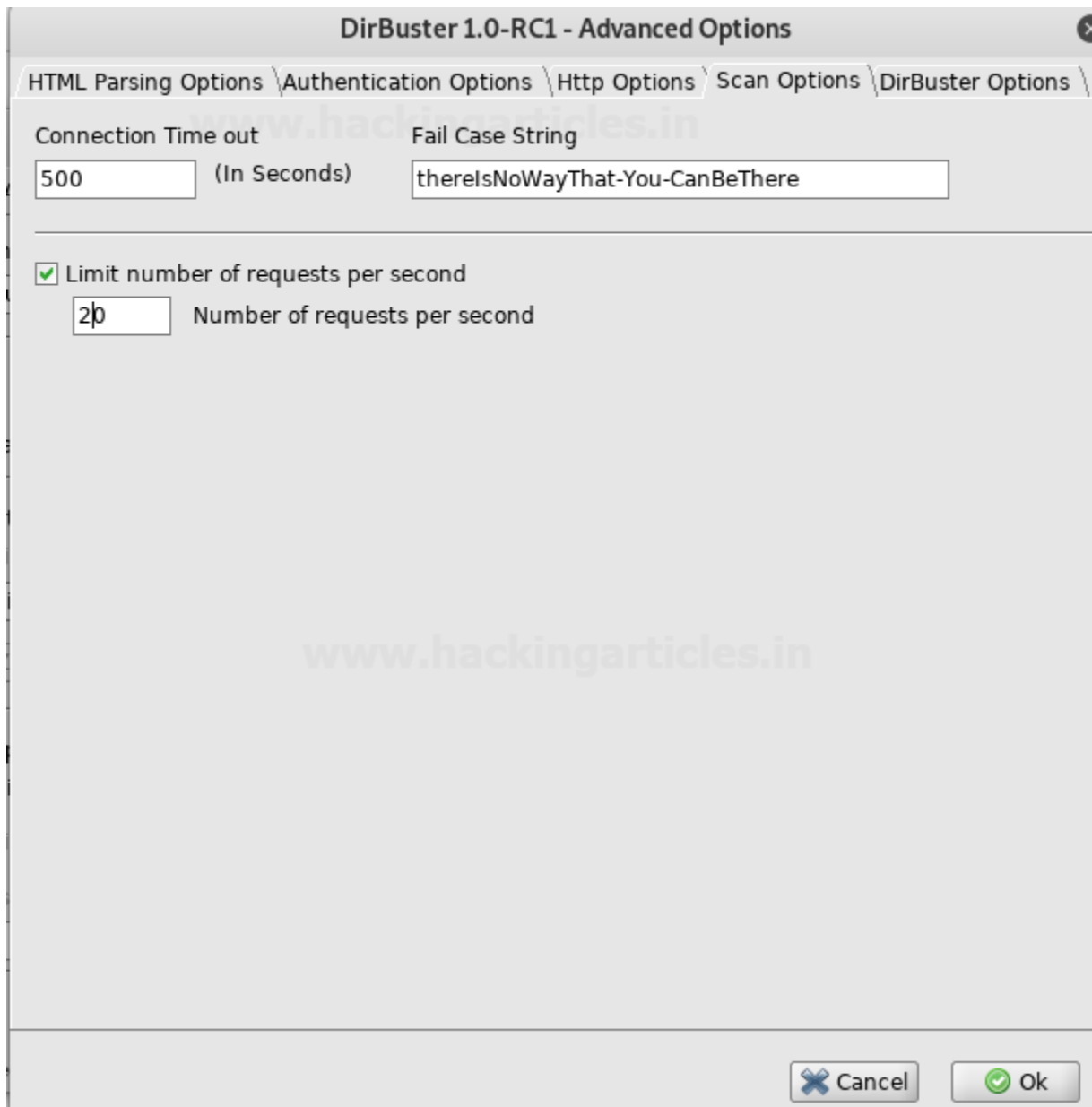


The screenshot shows the 'DirBuster 1.0-RC1 - Advanced Options' dialog box with the 'Scan Options' tab selected. The 'Connection Time out' is set to 30 (In Seconds) and the 'Fail Case String' is 'thereIsNoWayThat-You-CanBeThere'. The 'Limit number of requests per second' checkbox is unchecked, and the 'Number of requests per second' field is set to 50. The dialog box has 'Cancel' and 'Ok' buttons at the bottom right.

Field	Value
Connection Time out (In Seconds)	30
Fail Case String	thereIsNoWayThat-You-CanBeThere
Limit number of requests per second (checkbox)	Unchecked
Number of requests per second	50

We are setting Connection Time Out to 500, checking the Limit number of requests per second and setting that field to 20.





Once the test initiated, we will see the results. The scan was stopped to show the initial findings.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://testphp.vulnweb.com:80/

Scan Information Results - List View: Dirs: 5 Files: 11 Results - Tree View Errors: 0

Type	Found	Response	Size
Dir	/	200	4290
File	/index.php	200	196
File	/categories.php	200	196
File	/artists.php	200	196
File	/disclaimer.php	200	196
File	/cart.php	200	196
File	/guestbook.php	200	196
Dir	/AJAX/	200	196
File	/AJAX/index.php	200	196
File	/login.php	200	196
File	/userinfo.php	302	220
Dir	/Mod_Rewrite_Shop/	200	196
Dir	/hpp/	200	196
Dir	/images/	200	154

Current speed: 55 requests/sec (Select and right click for more options)  
Average speed: (T) 50, (C) 53 requests/sec  
Parse Queue Size: 0 Current number of running threads: 10  
Total Requests: 701/107037  Change  
Time To Finish: 00:33:26

Back Pause Stop Report

DirBuster Stopped /Mod\_Rewrite\_Shop/~fwadmin/

Once the scan is complete the actual findings can be seen.

**OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing**

File Options About Help

http://testphp.vulnweb.com:80/

Scan Information Results - List View: Dirs: 4 Files: 1 Results - Tree View Errors: 0

Type	Found	Response	Size
Dir	/	200	4290
Dir	/images/	200	154
Dir	/cgi-bin/	403	470
Dir	/admin/	200	154
Dir	/pictures/	200	154
File	/index.php	200	196
File	/categories.php	200	196

Current speed: 0 requests/sec (Select and right click for more options)

Average speed: (T) 21, (C) 20 requests/sec

Parse Queue Size: 0

Total Requests: 726/2205489

Current number of running threads: 100

Time To Finish: 1 Day

We hope you enjoy using this tool. It is a great tool that's a must in a pen tester's arsenal.

# JOIN OUR TRAINING PROGRAMS

