

Hacking Articles

Raj Chandel's Blog

Menu

[🏠 Home](#) » [Hacking Tools](#) » [Comprehensive Guide on Dirbuster Tool](#)

[Hacking Tools](#) , [Penetration Testing](#)

Comprehensive Guide on Dirbuster Tool

November 19, 2018 By Raj

In this article, we are focusing on the transient directory using Kali Linux tool Dibuster and trying to find hidden files and directories within a web server.

Table of Content

- What is DirBuster
- Default Mode
- GET Request Method
- Pure Brute Force (Numeric)
- Single Sweep (Non-recursive)
- Targeted Start
- Blank Extensions
- Search by File Type (.txt)
- Changing the DIR List
- Following Redirects
- Attack Through Proxy
- Adding File Extensions
- Evading Detective Measures (Requests Per Second)

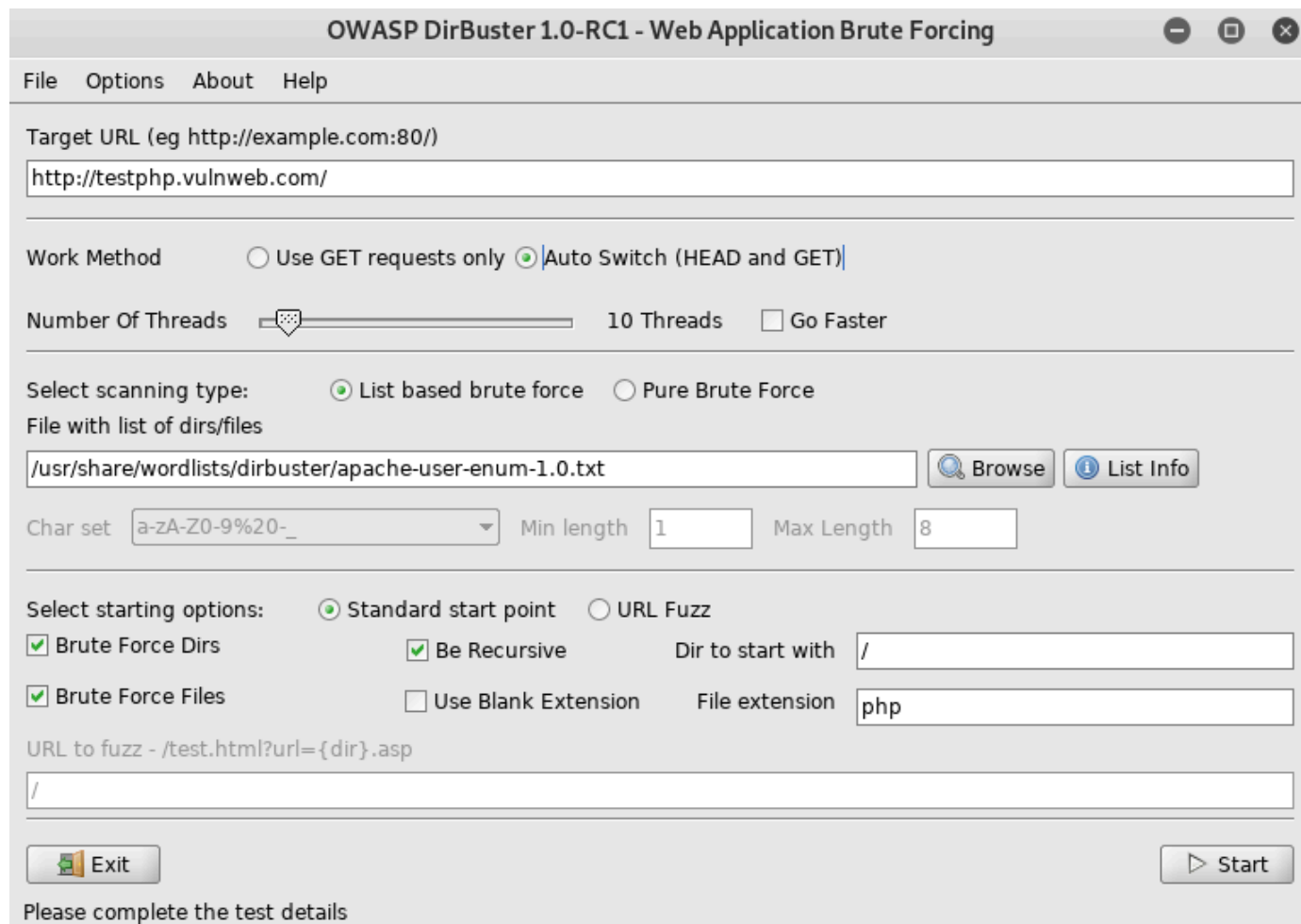
What is DirBuster

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 - Web Application Brute Forcing application window. The interface includes a menu bar (File, Options, About, Help) and a main configuration area. The Target URL field is set to `http://testphp.vulnweb.com/`. The Work Method is set to **Auto Switch (HEAD and GET)**. The Number Of Threads is set to 10 Threads. The Select scanning type is set to **List based brute force**. The File with list of dirs/files is set to `/usr/share/wordlists/dirbuster/apache-user-enum-1.0.txt`. The Char set is set to `a-zA-Z0-9%20-_%`, Min length is 1, and Max Length is 8. The Select starting options are set to **Standard start point**. The Brute Force Dirs, Brute Force Files, and Be Recursive checkboxes are checked. The Dir to start with is set to `/` and the File extension is set to `php`. The URL to fuzz is set to `/test.html?url={dir}.asp`. The Exit and Start buttons are visible at the bottom.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

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 10 Threads ☐ Go Faster

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`

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

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.

The screenshot shows the OWASP DirBuster 1.0-RC1 interface. The title bar reads "OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing". The menu bar includes "File", "Options", "About", and "Help". The address bar shows "http://testphp.vulnweb.com:80/". Below the address bar, there are tabs for "Scan Information", "Results - List View: Dirs: 5 Files: 11", "Results - Tree View", and "Errors: 0". The main area displays a table of scan results:

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

Below the table, the following statistics are displayed:

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

At the bottom, there are buttons for "Back", "Pause", "Stop", and "Report". The status bar at the bottom indicates "DirBuster Stopped" and the current path is "/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.

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

DirBuster Stopped /Mod_Rewrite_Shop/~fwadmin/

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/)

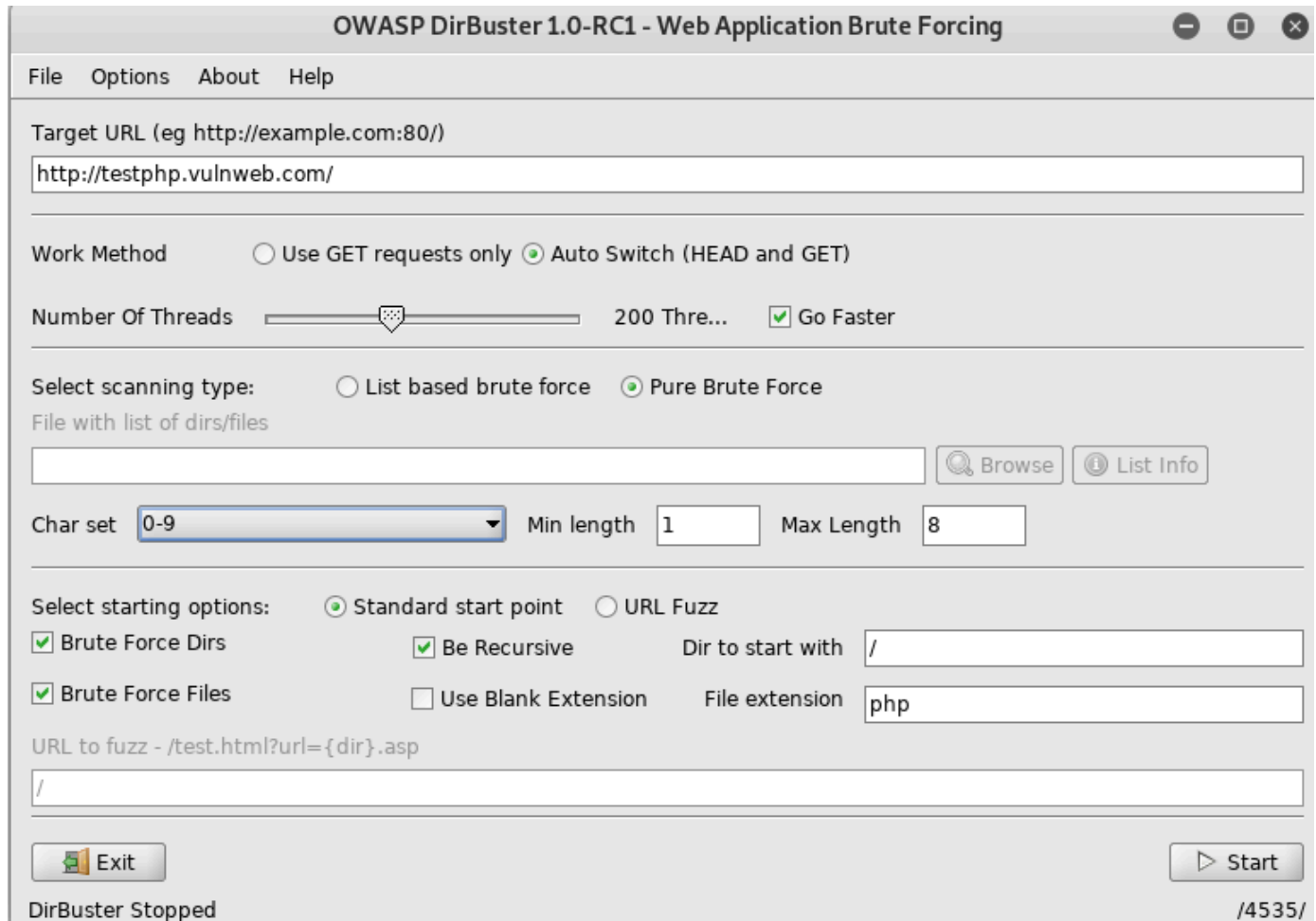
Directory Structure	Response Code	Response Size
/	200	4290
index.php	200	4290
artists.php	200	4655
categories.php	200	5454
disclaimer.php	200	4861
cart.php	200	4234
guestbook.php	200	4725
AJAX	200	4430
login.php	200	4865
userinfo.php	302	234
Mod_Rewrite_Shop	200	1171
hpp	200	399

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
Time To Finish: 00:01:51
Current number of running threads: 200

Starting dir/file list based brute forcing /Mod_Rewrite_Shop/images/~axe/

Pure Brute Force (Numeric)

DirBuo performs 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 limit are set.



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

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 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

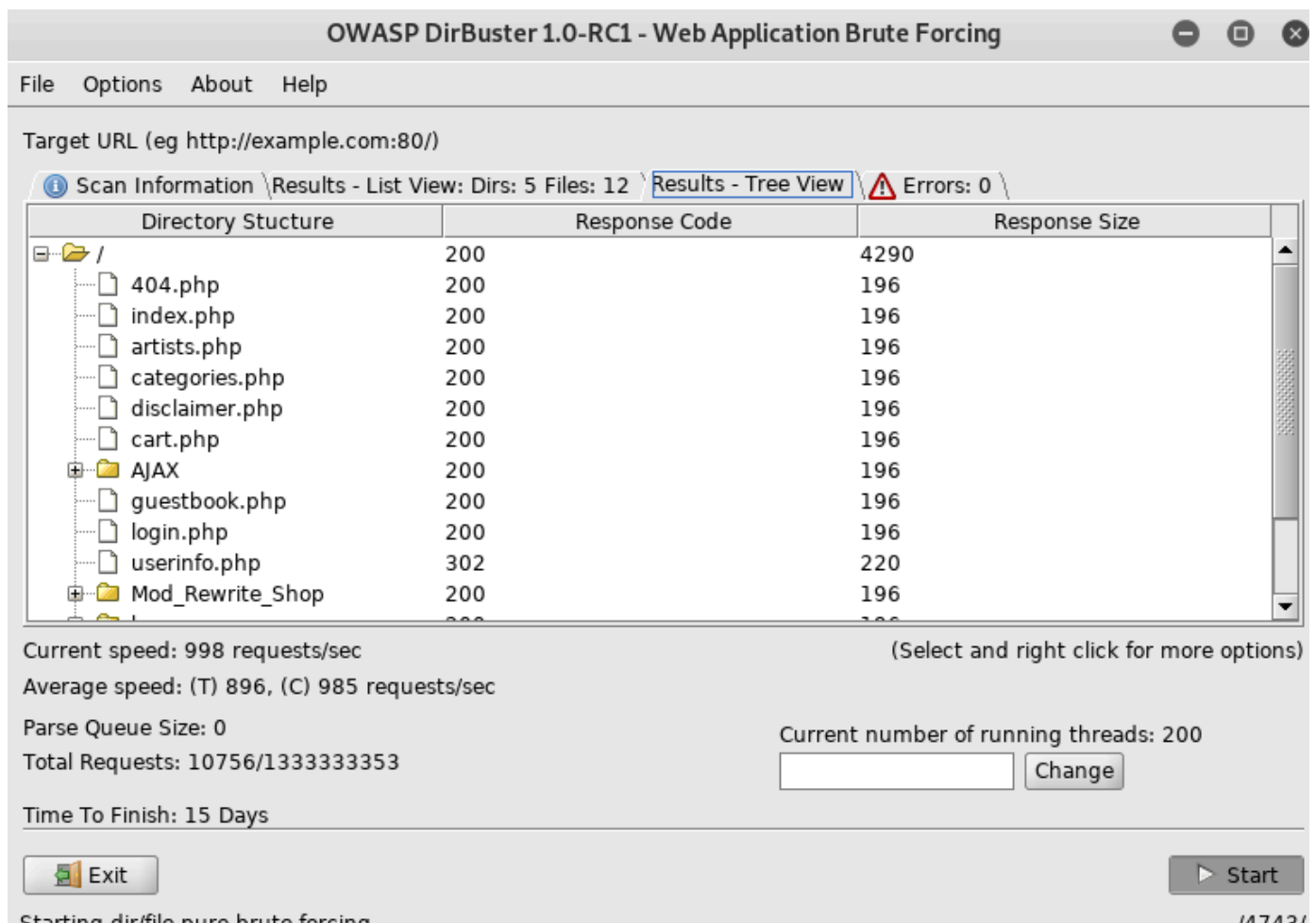
☒ Brute Force Dirs ☒ Be Recursive Dir to start with

☒ Brute Force Files ☐ Use Blank Extension File extension

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

DirBuster Stopped /4535/

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

FileOptionsAboutHelp

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

Browse

List Info

Char set

a-zA-Z0-9%20_-

Min lengthMax 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

Exit

Start

Please complete the test details

In the Results – ListView we can see findings.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

FileOptionsAboutHelp

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

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

Parse Queue Size: 0

Total Requests: 10734/17857

Time To Finish: 00:00:07

Back

Pause

Stop

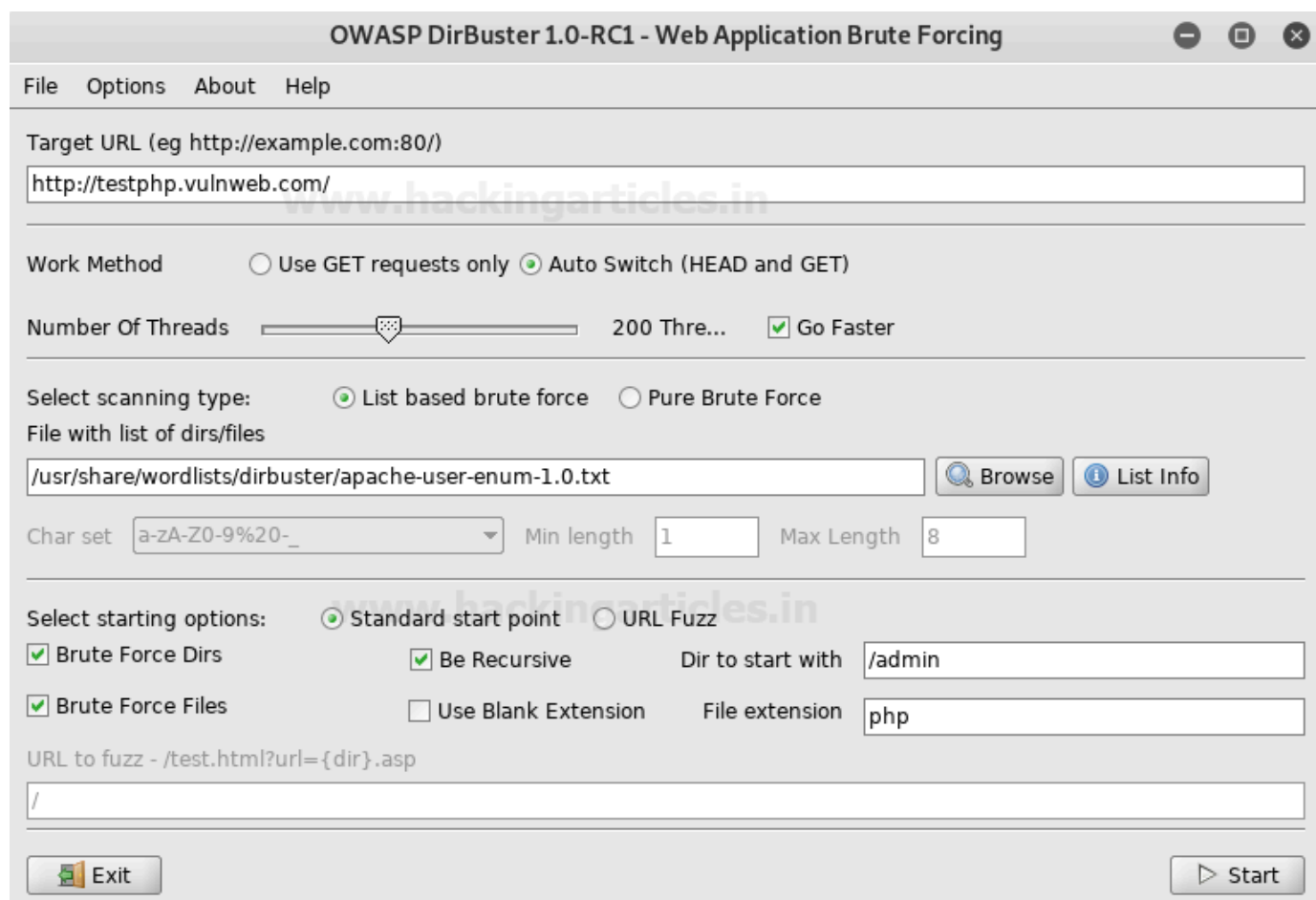
Current number of running threads: 200

Change

Report

Targeted Start

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



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

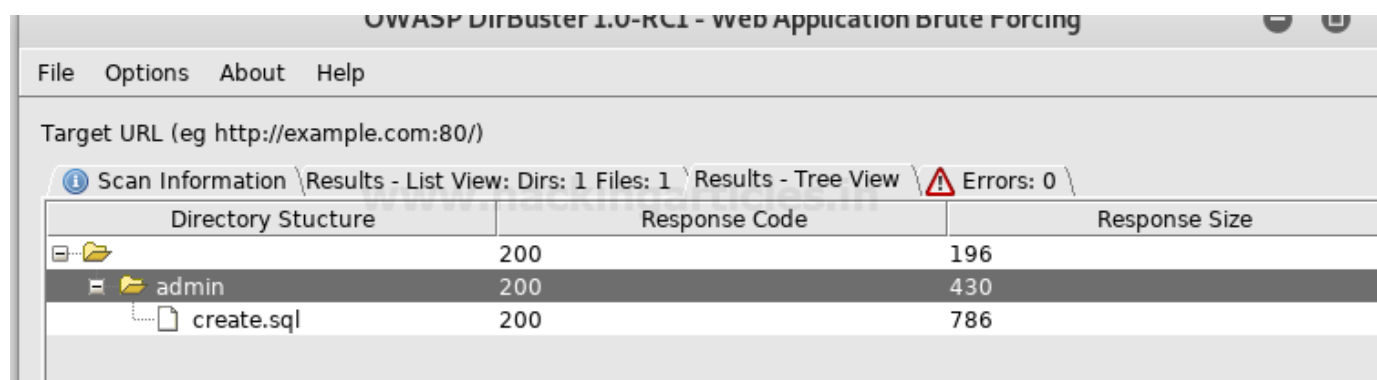
Select starting options: ☒ Standard start point ☐ URL Fuzz

☒ 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


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: 1 Files: 1 \ Results - Tree View \  Errors: 0 \

Directory Stucture	Response Code	Response Size
	200	196
 admin	200	430
 create.sql	200	786

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.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

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 200 Thre... ☒ Go Faster

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

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

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

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

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

Testing for	Progress	Pause	Stop
dirs in /	18%	<input type="button" value="Pause"/>	<input type="button" value="Stop"/>
files in / with no extention	19%	<input type="button" value="Pause"/>	<input type="button" value="Stop"/>
files in / with extention .php	27%	<input type="button" value="Pause"/>	<input type="button" value="Stop"/>
dirs in /AJAX/	3%	<input type="button" value="Pause"/>	<input type="button" value="Stop"/>
files in /AJAX/ with no extention	2%	<input type="button" value="Pause"/>	<input type="button" value="Stop"/>
files in /AJAX/ with extention .php	2%	<input type="button" value="Pause"/>	<input type="button" value="Stop"/>
dirs in /Mod_Rewrite_Shop/	1%	<input type="button" value="Pause"/>	<input type="button" value="Stop"/>

Search by File Type (.txt)

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

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

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

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

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

Results - List View: Dirs: 5 Files: 11 \Results - Tree View \

Testing for dirs in /	32%	<input type="button" value="List"/> <input type="button" value="Stop"/>
Testing for files in / with extension .txt	42%	<input type="button" value="List"/> <input type="button" value="Stop"/>
Testing for dirs in /AJAX/	10%	<input type="button" value="List"/> <input type="button" value="Stop"/>
Testing for files in /AJAX/ with extension .txt	10%	<input type="button" value="List"/> <input type="button" value="Stop"/>
Testing for dirs in /Mod_Rewrite_Shop/	8%	<input type="button" value="List"/> <input type="button" value="Stop"/>
Testing for files in /Mod_Rewrite_Shop/ with extension .txt	9%	<input type="button" value="List"/> <input type="button" value="Stop"/>
Testing for dirs in /hpp/	9%	<input type="button" value="List"/> <input type="button" value="Stop"/>

Current speed: 932 requests/sec (Select and right click for more options)

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.

The screenshot shows the OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing application window. The interface includes a menu bar (File, Options, About, Help) and a main configuration area. The 'Target URL' field is empty. The 'Work Method' section has two radio buttons: 'Use GET requests only' and 'Auto Switch (HEAD and GET)', with the latter selected. The 'Number Of Threads' is set to 200, with a 'Go Faster' checkbox. The 'Select scanning type' section has two radio buttons: 'List based brute force' (selected) and 'Pure Brute Force'. Below this, the 'File with list of dirs/files' field contains the path '/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt', with 'Browse' and 'List Info' buttons. The 'Char set' is set to 'a-zA-Z0-9%20-', 'Min length' is 1, and 'Max Length' is 8. The 'Select starting options' section has two radio buttons: 'Standard start point' (selected) and 'URL Fuzz'. There are four checkboxes: 'Brute Force Dirs' (checked), 'Be Recursive' (checked), 'Brute Force Files' (checked), and 'Use Blank Extension' (unchecked). The 'Dir to start with' field contains '/', and the 'File extension' field contains 'php'. The 'URL to fuzz' field contains the template '/test.html?url={dir}.asp'. At the bottom, there are 'Exit' and 'Start' buttons, and a message 'Please complete the test details'.

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 Thre... ☐ Go Faster

Select scanning type: ☒ List based brute force ☐ Pure Brute Force

File with list of dirs/files

/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Char set Min length Max Length

Select starting options: ☒ Standard start point ☐ URL Fuzz

☒ Brute Force Dirs ☒ Be Recursive Dir to start with

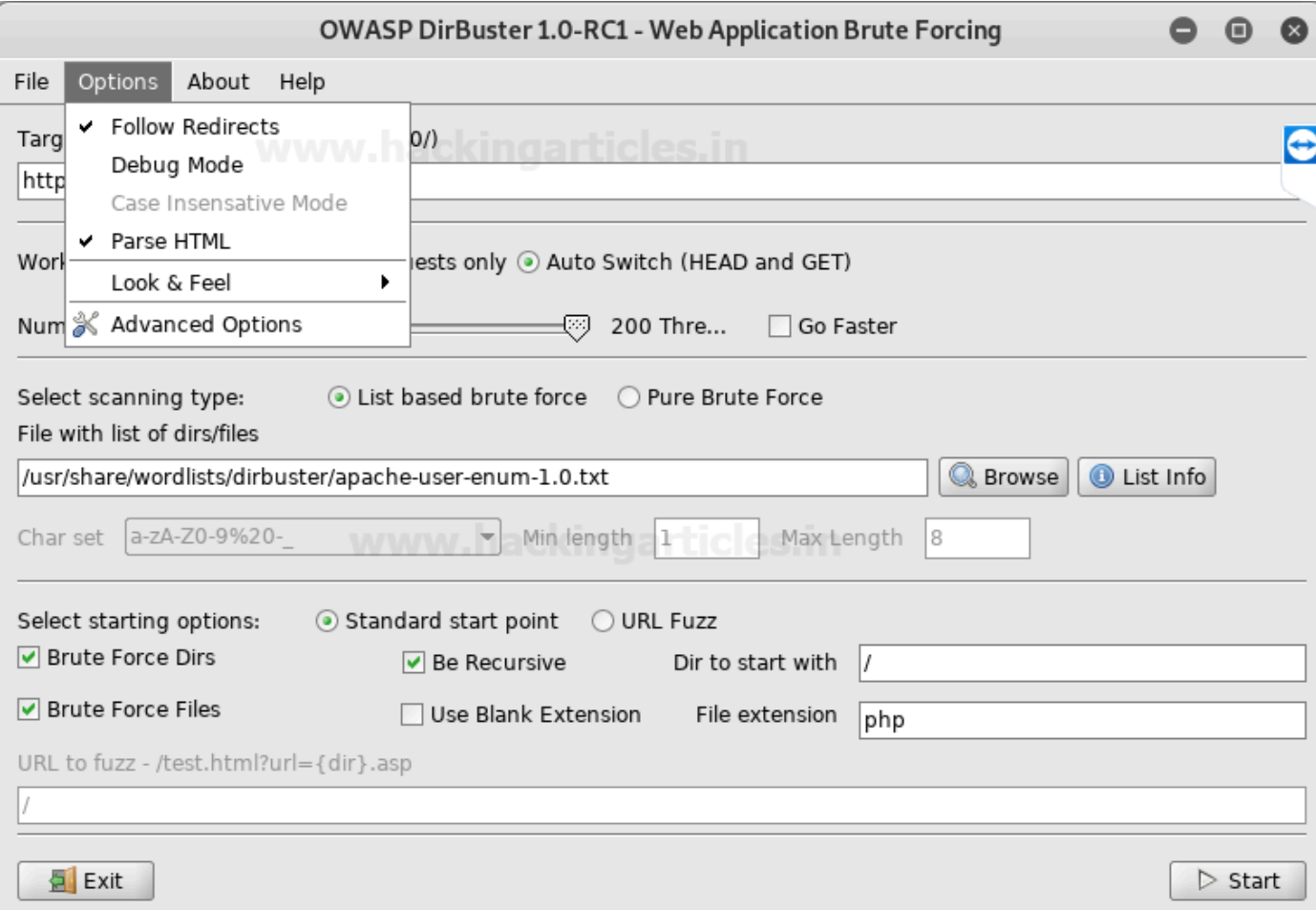
☒ Brute Force Files ☐ Use Blank Extension File extension

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

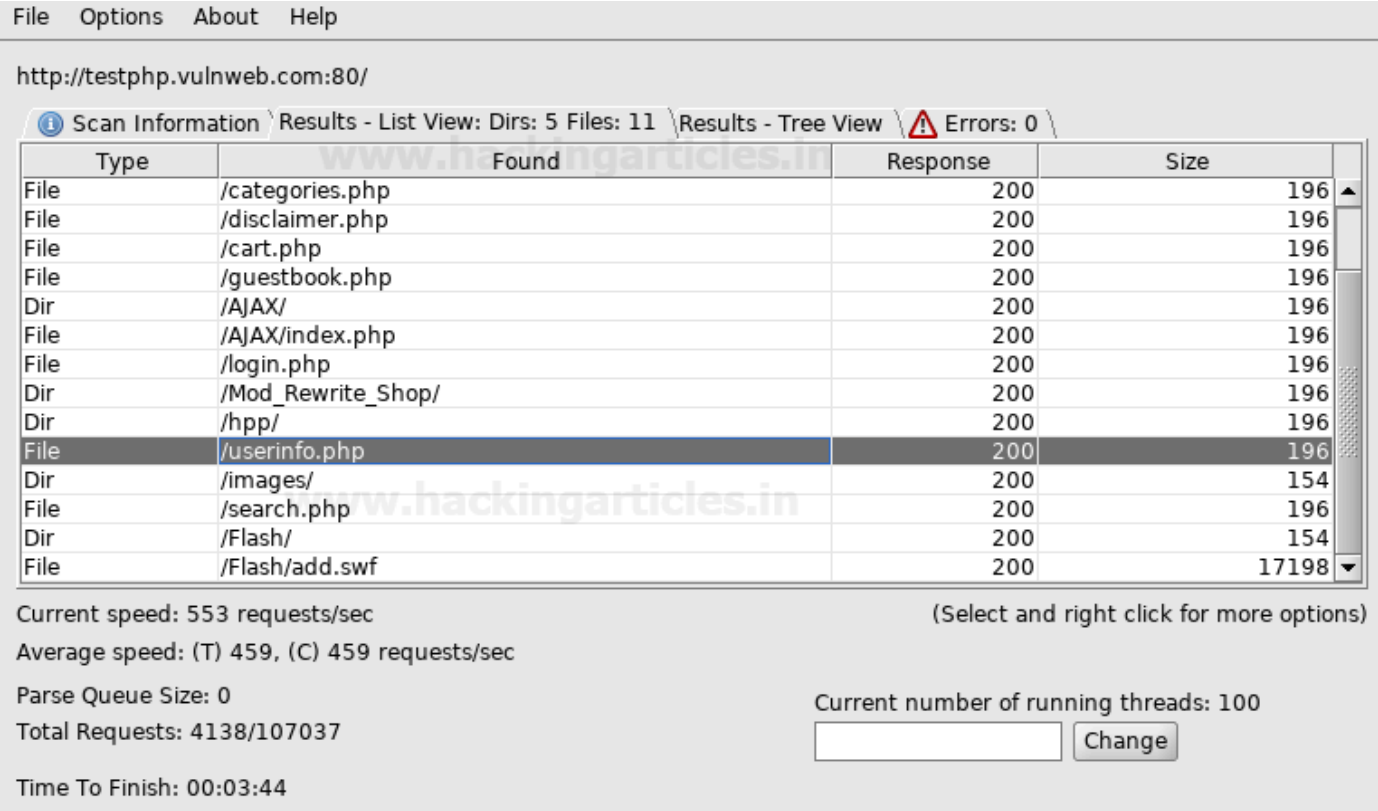
Please complete the test details

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.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

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

Scan Information \ Results - List View: Dirs: 9 Files: 19 \ Results - Tree View \ Errors: 0

Directory Structure	Response Code	Response Size
cgi-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

Current speed: 464 requests/sec (Select and right click for more options)

Average speed: (T) 500, (C) 526 requests/sec

Parse Queue Size: 0

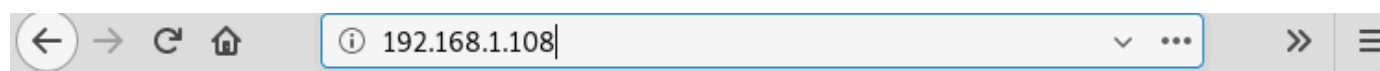
Total Requests: 10014/4410974

Current number of running threads: 100

Change

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

Apache

We set the IP in DirBuster as the attack target.

The screenshot shows the OWASP DirBuster 1.0-RC1 interface. The title bar reads "OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing". The menu bar includes "File", "Options", "About", and "Help". The main configuration area is divided into several sections:

- Target URL (eg http://example.com:80/)**: A text box containing "http://192.168.1.108/".
- Work Method**: Two radio buttons, "Use GET requests only" (unselected) and "Auto Switch (HEAD and GET)" (selected).
- Number Of Threads**: A slider set to "200 Thre..." and a checkbox "Go Faster" (unchecked).
- Select scanning type:** Two radio buttons, "List based brute force" (selected) and "Pure Brute Force" (unselected).
- File with list of dirs/files**: A text box containing "/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt", with "Browse" and "List Info" buttons to its right.
- Char set**: A dropdown menu showing "a-zA-Z0-9%20-_", with "Min length" (1) and "Max Length" (8) input boxes.
- Select starting options:** Two radio buttons, "Standard start point" (selected) and "URL Fuzz" (unselected).
- Brute Force Dirs**: A checked checkbox, with "Be Recursive" (checked) and "Dir to start with" ("/") options.
- Brute Force Files**: A checked checkbox, with "Use Blank Extension" (unchecked) and "File extension" ("php") options.
- URL to fuzz - /test.html?url={dir}.asp**: A text box containing "/".

At the bottom, there are "Exit" and "Start" buttons.

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

Custom HTTP Headers

Header	Value
--------	-------

Add New Custom HTTP Header

:

Http User Agent

Proxy Information & Authentification

☒ 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

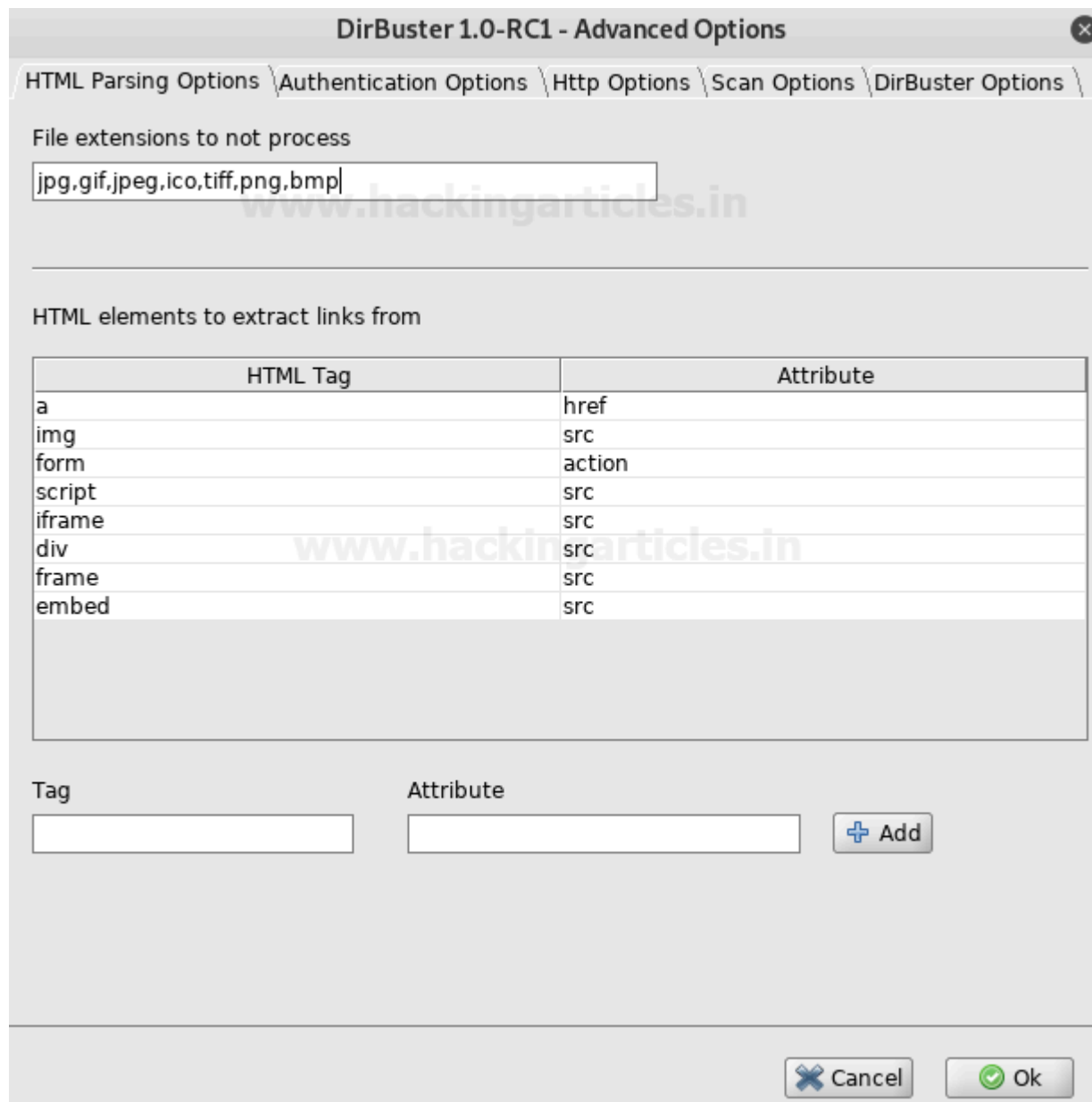
Type	Found	Response	Size
Dir	/	200	3784
Dir	/error/	403	429
Dir	/icons/	200	344
Dir	/error/include/	403	429
Dir	/icons/small/	200	344
Dir	/blog/	200	410
Dir	/blog/wp-content/	200	331
File	/blog/wp-content/index.php	200	331
Dir	/blog/wp-content/themes/	200	331
Dir	/blog/wp-content/uploads/	403	429
File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



The screenshot shows the 'DirBuster 1.0-RC1 - Advanced Options' dialog box with the 'HTML Parsing Options' tab selected. The 'File extensions to not process' field contains 'jpg,gif,jpeg,ico,tiff,png,bmp'. Below this is a table for 'HTML elements to extract links from'.

HTML Tag	Attribute
a	href
img	src
form	action
script	src
iframe	src
div	src
frame	src
embed	src

At the bottom, there are input fields for 'Tag' and 'Attribute', an '+ Add' button, and 'Cancel' and 'Ok' buttons at the very bottom.

We will delete jpeg in this instance and click OK.

DirBuster 1.0-RC1 - Advanced Options

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

File extensions to not process

gif,ico,tiff,png,bmp

www.hackingarticles.in

HTML elements to extract links from

HTML Tag	Attribute
a	href
img	src
form	action
script	src
iframe	src
div	src
frame	src
embed	src

Tag

Attribute

+ Add

Cancel

Ok

In the File Extension filed we will type in “jpeg” to explicitly tell DirBuster to look for .jpeg format files.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

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 200 Thre... ☐ Go Faster

Select scanning type: ☒ List based brute force ☐ Pure Brute Force

File with list of dirs/files

/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

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

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

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: 6 Results - Tree View Errors: 0

Testing for dirs in /	0%	<input type="button" value="Pause"/>	<input type="button" value="Stop"/>
Testing for files in / with extension .jpeg	0%	<input type="button" value="Pause"/>	<input type="button" value="Stop"/>
Testing for dirs in /images/	0%	<input type="button" value="Pause"/>	<input type="button" value="Stop"/>
Testing for files in /images/ with extension .jpeg	0%	<input type="button" value="Pause"/>	<input type="button" value="Stop"/>
Testing for dirs in /cgi-bin/	0%	<input type="button" value="Pause"/>	<input type="button" value="Stop"/>
Testing for files in /cgi-bin/ with extension .jpeg	0%	<input type="button" value="Pause"/>	<input type="button" value="Stop"/>
Testing for dirs in /admin/	0%	<input type="button" value="Pause"/>	<input type="button" value="Stop"/>

Current speed: 532 requests/sec (Select and right click for more options)

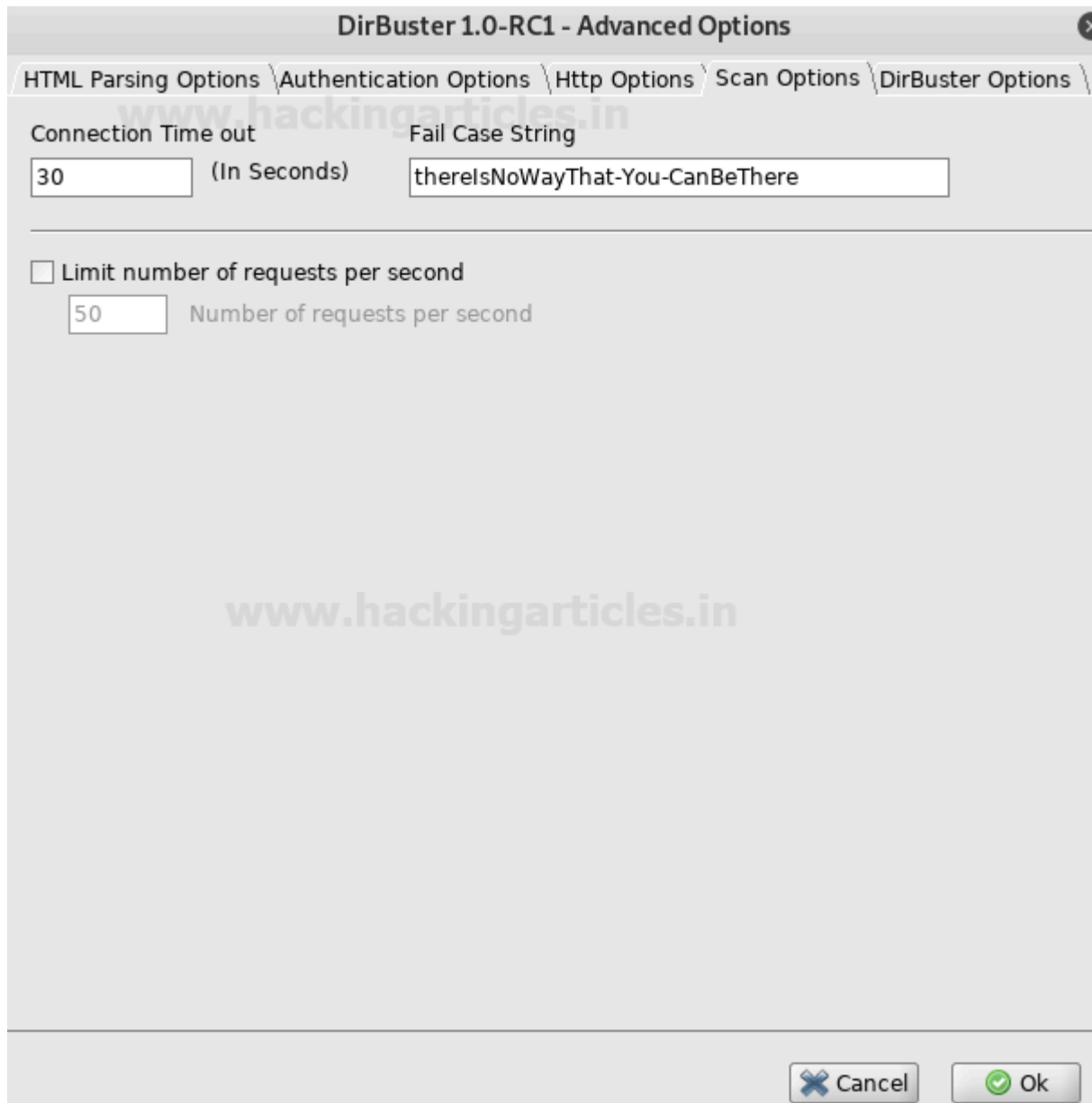
Average speed: (T) 410, (C) 410 requests/sec

Parse Queue Size: 0 Current number of running threads: 100

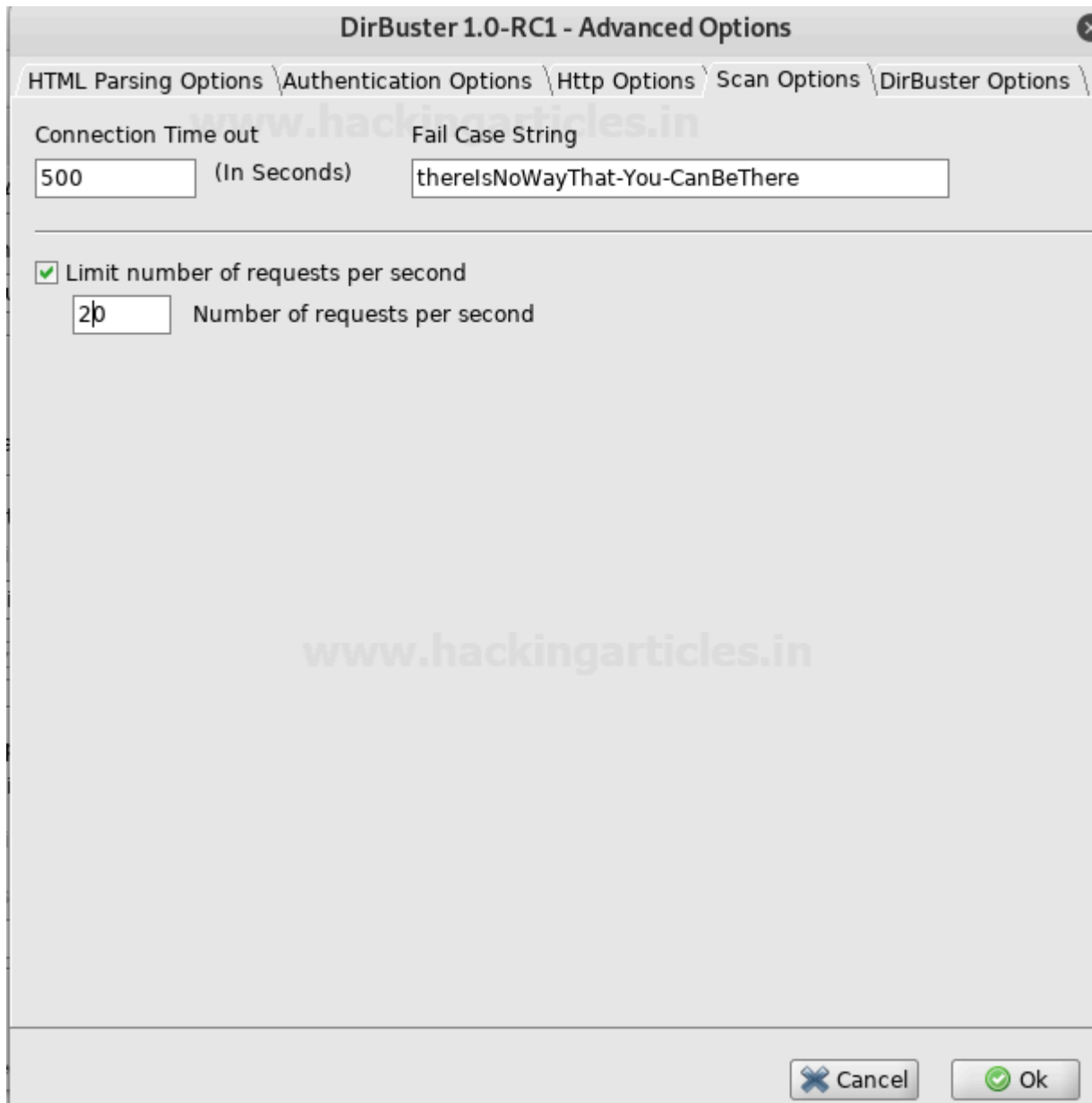
Total Requests: 2050/2646589

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.



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

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/

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

Change

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

Stay tuned for more articles on the latest and greatest in hacking.