

WIGS

MAKS UP

A DETAILED GUIDE ON DORBUSTER

HOW TO BE A DETECTIVE

In 10 Lessons

D

WWW.HACKINGARTICLES.IN

6

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 Dibuster 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.

	OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing	•	•	⊗	
File Options About He	elp				
Target URL (eg http://exam	nple.com:80/)				
http://testphp.vulnweb.co	m/				
Work Method Ous	e GET requests only ③ Auto Switch (HEAD and GET)				
Number Of Threads 🖃	10 Threads 🗌 Go Faster				
Select scanning type: File with list of dirs/files	Iist based brute force				
/usr/share/wordlists/dirbus	ter/apache-user-enum-1.0.txt	nfo			
Char set a-zA-Z0-9%20 Min length 1 Max Length 8					
Select starting options:	Standard start point O 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				
/					
Exit			Start	t	
Please complete the test de	etails				

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	000
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 S	ize
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		. 10
Time To Finish, 00-22-26		
Time To Finish: 00:33:26		
Back 00 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.



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 I 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 a-zA-Z0-9%20 Min length 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					
/					
Exit	> Sta	rt			
DirBuster Stopped /Mod_Rewrite_Shop/-	fwadı	min/			

In the Results – Tree View we can see findings.



OWASP D	irBuster 1.0-RC1 - Web Applicatio	n Brute Forcing 🛛 🖨 🕲 🔇
File Options About Help		
Target URL (eg http://example.com:80/)		
Iscan Information Results - List Vie	w: Dirs: 6 Files: 15 Results - Tree Vie	W A Errors: 0
Directory Stucture	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
	<u> </u>	
Current speed: 898 requests/sec		(Select and right click for more options)
Average speed: (T) 856, (C) 943 reques	ts/sec	
Parse Queue Size: 14083	Curr	ent number of running threads: 200
Total Requests: 19696/124890		Change
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.



	OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing	0		8	
File Options About	Help				
Target URL (eg http://e	example.com:80/)				
http://testphp.vulnwe	p.com/				
Work Method) Use GET requests only ④ Auto Switch (HEAD and GET)				
Number Of Threads	200 Thre 🗹 Go Faster				
Select scanning type: O List based brute force Image: Pure Brute Force File with list of dirs/files Image: Pure Brute Force Image: Pure Brute Force Char set 0-9 Image: Pure Brute Force Image: Pure Brute Force Min length 1 Max Length 8					
Select starting options	• • • • • • • • • • • • • • • • • • •				
Brute Force Dirs	✓ Be Recursive Dir to start with /				
Brute Force Files	Use Blank Extension File extension php				
URL to fuzz - /test.htm	?url={dir}.asp				
/					
Exit	(⊳	Star	t	
DirBuster Stopped			/45	35/	

In the Results – Tree View we can see findings.



OWASP	DirBuster 1.0-RC1 - Web Applic	ation Brute Forcing 🗢 💿 🛽
File Options About Help		
Target URL (eg http://example.com:80,)	
🕕 🕕 Scan Information \Results - List Vi	ew: Dirs: 5 Files: 12 ⁾ Results - Tre	e View 🕅 🚹 Errors: 0 🔪
Directory Stucture	Response Code	Response Size
□ 🍃 /	200	4290
	200	196
index.php	200	196
artists.php	200	196 555
🗋 categories.php	200	196
disclaimer.php	200	196
cart.php	200	196
🖶 🖆 AJAX	200	196
guestbook.php	200	196
login.php	200	196
userinfo.php	302	220
Mod_Rewrite_Shop	200	196
		(Coloct and right click for more entions)
current speed: 998 requests/sec		(select and right click for more options)
Average speed: (1) 896, (C) 985 reque	sts/sec	
Parse Queue Size: 0		Current number of running threads: 200
Total Requests: 10756/1333333353		Change
Time To Finish: 15 Days		
Exit		► Start
Storting diritilo puro bruto torcing		12474

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/)		
http://testphp.vulnweb.com/		
Work Method Ouse GET requests only (a) Auto Switch (HEAD and GET)		
Number Of Threads 200 Thre V 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-ZO-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		
Exit	Star	t
Please complete the test details		

In the Results – ListView we can see findings.



	OWASP DirBuster 1.0-RC1 - Web Applicat	ion Brute Forcing	•		8
File Options	About Help				
http://testphp	.vulnweb.com:80/				
🕠 Scan Infe	ormation Results - List View: Dirs: 0 Files: 11 Results - Tree V	/iew \ 🔥 Errors: 0 \			
Туре	Found	Response	Size		
Dir	/	200	4	290	
File	/index.php //// ackinganticles.in	200		196	
File	/artists.php	200		196	
File	/categories.php	200		196	
File	/disclaimer.php	200		196	33
File	/cart.php	200		196	
File	/guestbook.php	200		196	
Dir	/AJAX/	200		196	333
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	I: 746 requests/sec	(Select and rig	ht click for more	optio	ns)
Average spee	d: (T) 825, (C) 897 requests/sec				
Parse Queue S	Size: 0 Cu	rrent number of runnin	iq threads: 200		
Total Request	s: 10734/17857	C	hange:		
Time To Finish	n: 00:00:07				
🖨 Back	Pause Stop		Re	port	

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.



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 Ouse GET requests only (a) 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 a-zA-Z0-9%20 Min length 1 Max Length 8
Select starting options:
✓ Brute Force Dirs ✓ Be Recursive Dir to start with /admin
Image: Brute Force Files Use Blank Extension File extension php
URL to fuzz - /test.html?url={dir}.asp
Exit > Start

In the Results – Tree View we can see findings.

UVVAS	P DIFBUSTER T.O-KCT - We	Application Brute Forcing		
File Options About Help				
Target URL (eg http://example.com:8	30/) View: Dirs: 1 Files: 1 `Result	s - Tree View \ 🕂 Errors: 0 \		
Directory Stucture	Response	Code	Response Size	
B	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.



			OWA	SP DirBuster 1.0-RC1 -	OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing					
File	Options	About	Help							
Targ	get URL (eg	g http://e	xample.com	:80/)						
htt	p://testphp	.vulnweb	.com/							
			WWW.	nackingarud	les.m					
Wor	k Method	С	Use GET re	quests only 💿 Auto Swit	ch (HEAD and GET)	l de la construcción de la constru				
Nun	nber Of Thi	reads 🛛		200) Thre 🔽 Go Fa	aster				
Sele	ect scannin	g type:	 List 	based brute force 🔾	Pure Brute Force					
File	with list of	dirs/files								
/us	r/share/wor	rdlists/dir	buster/apach	ne-user-enum-1.0.txt		🔍 Browse 🕕 List	Info			
Cha	r set a-zA	A-Z0-9%2	0	Min length	1 Max Le	ength 8				
Sele	ect starting	options:	 Stan 	dard start point 🛛 UF	L Fuzz					
💌 B	rute Force	Dirs		Be Recursive	Dir to start with	/				
V B	rute Force	Files		Use Blank Extension	File extension	php				
URL	. to fuzz - /t	est.html	url={dir}.a	sp						
/										
	Exit							Star	t	

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

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing	•	▣	8
File Options About Help			
http://testphp.vulnweb.com:80/			
🕕 🕕 Scan Information \Results - List View: Dirs: 5 Files: 11 \Results - Tree View \ 🔥 Errors: 0 \			
Testing for dirs in /			•
Testing for files in / with no extention 19%			
Testing for files in / with extention .php 27%			<u> </u>
Testing for dirs in /AJAX/ WWW.hackingarticles			
Testing for files in /AJAX/ with no extention 2%			
Testing for files in /AJAX/ with extention .php 2%			
Testing for dirs in /Mod_Rewrite_Shop/ 1%			•

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."



OWASP DirBuster 1.0-RC1 - Web Application	n Brute Forcing 🗧 🙃	8
File Options About Help		
Target URL (eg http://example.com:80/)		
http://testphp.vulnweb.com/		
Work Method Ouse GET requests only Auto Switch (HEAD and GET) 	т)	_
Number Of Threads 200 Thre V Go	Faster	
Select scanning type: $\hfill \ensuremath{{\circ}}$ List based brute force $\hfill \ensuremath{{\circ}}$ Pure Brute Force File with list of dirs/files		
/usr/share/wordlists/dirbuster/apache-user-enum-1.0.txt	🔍 Browse 🕕 List Info	
Char set a-zA-Z0-9%20 Min length 1 Max I	Length 8	
Select starting options: Standard start point URL Fuzz 		
✓ Brute Force Dirs ✓ Be Recursive Dir to start with	h /	
✓ Brute Force Files Use Blank Extension File extension	n txt	
URL to fuzz - /test.html?url={dir}.asp		
Exit	▷ Start	
We can see the processing happen and DirBuster testing to find di	rectories with a .txt extension.	
OWASP DirBuster 1.0-RC1 - Web Application	n Brute Forcing 🔹 🕒	8
File Options About Help		
http://testphp.vulnweb.com:80/		
Scan Information Results - List View: Dirs: 5 Files: 11 \Results - Tree View	w 🕅 Errors: 0 \	
Testing for dirs in / www.hackingarticles.in	32%	
Testing for files in / with extention .txt	42%	100000
Testing for dirs in /AJAX/	10%	3000000
Testing for files in /AJAX/ with extention .txt	10%	4
Testing for dirs in /Mod_Rewrite_Shop/ 	8%	
Testing for files in /Mod_Rewrite_Shop/ with extention .txt	9% 🔲 🗆	
Testing for dirs in /hpp/	9%	•
Current speed: 932 requests/sec	(Select and right click for more option	is)

Current speed: 932 requests/sec



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.

	DirBuster 1.0-RC1 - Advanced Options	8
HTML Parsing Options \setminus A	withentication Options \langle Http Options \langle Scan Options \rangle DirBus	ter Options \setminus
Allow DirBuster to ch Check Now	eck for updates	
Default settings (DirBus	ter must be restarted for settings to be applied)	
Number of threads:	200	
Dir list to use:	/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt	🔍 Browse
File extensions to test:	php	
	💥 Cancel	🕝 Ok

We can see the word list is now set.



	OWASP DirBuster 1.0-RC1 - Web Application Brute Forcin	g – 🗆 🗙			
File Options About H	elp				
Target URL (eg http://exan	Target URL (eg http://example.com:80/)				
W	ww.hackingarticles.in				
Work Method 🛛 🔾 Us	e GET requests only Auto Switch (HEAD and GET)				
Number Of Threads	200 Thre 🗌 Go Faster				
Select scanning type: File with list of dirs/files	Select scanning type: List based brute force Pure Brute Force File with list of dirs/files				
/usr/share/wordlists/dirbus	ter/directory-list-2.3-medium.txt	3rowse 🕕 List Info			
Char set a-zA-Z0-9%20	▼ Min length 1 Max Length 8				
	www.hackingarticles.in				
Select starting options:	Standard start point O 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					
Start					
Please complete the test de	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.



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing	8		
File Options About Help			
Targ Follow Redirects Debug Mode Case Insensative Mode 0/) Insensative Mode Insensative Mode Insensative Mode Insensative Mode Insensative Mode 	0		
Work Look & Feel			
Num 🔏 Advanced Options 🔅 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 Browse ① List Info			
Char set a-zA-Z0-9%20 Min length 1 tick Max Length 8			
Select starting options: Standard start point URL Fuzz 			
Image: Brute Force Dirs Image: Be Recursive Dir to start with			
Image: Brute Force Files Use Blank Extension File extension php			
URL to fuzz - /test.html?url={dir}.asp /			
Exit D Sta	rt		

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

Type	Found	Response	Size
ile	/categories.php	200	196
ile	/disclaimer.php	200	196
ile	/cart.php	200	196
ile	/guestbook.php	200	196
Dir	/AJAX/	200	196
ile	/AJAX/index.php	200	196
ile	/login.php	200	196
Dir	/Mod_Rewrite_Shop/	200	196
Dir	/hpp/	200	196
ile	/userinfo.php	200	196
Dir	/images/	200	154
ile	/search.php	200	196
Dir	/Flash/	200	154
ile	/Flash/add.swf	200	17198

Time To Finish: 00:03:44



Results in the Tree View.

OWASP D	irBuster 1.0-RC1 - Web Application	n Brute Forcing 🕒 🕒 😣
File Options About Help		
http://testphp.vulnweb.com:80/		
I Scan Information Results - List Vie	w: Dirs: 9 Files: 19 Results - Tree Vie	w \ 🕂 Errors: 0 \
Directory Stucture	Response Code	Response Size
🖶 🖆 cgi-bin	403	470
art.php	200 carries in	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 reques	ts/sec	
Parse Queue Size: 0	Curre	ent number of running threads: 100
Total Requests: 10014/4410974		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.

(←) → 健 @	(i) 192.168.1.108	~ ***	»	≡
	The second se			

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

<u>192.168.1.108</u> Apache

We set the IP in DirBuster as the attack target.



	OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing				
File Options About	Help				
Target URL (eg http://example.com:80/)					
http://192.168.1.108/					
Work Method	Jse GET requests only ④ Auto Switch (HEAD and GET)				
Number Of Threads 🛛 💳	200 Thre 🗌 Go Faster				
Select scanning type: File with list of dirs/files	● List based brute force ○ Pure Brute Force				
/usr/share/wordlists/dirb	uster/directory-list-2.3-medium.txt	Info			
Char set a-zA-Z0-9%20	Min length 1 Max Length 8				
Select starting options:	Standard start point O 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					
/					
Exit		\triangleright	Star	t	

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	jarticles.in		
Header	Value		
Add New Custom HTTP Header			
:	✿ Add		
Http User Agent			
DirBuster-1.0-RC1 (http://www.owasp.org/index.	php/Category:OWASP_DirBuster_Project)		
www.hackinga	rticles.in		
Proxy Information & Authentifcation			
Run Through a Proxy			
Host Port			
192.168.1.108 3129			
Use Proxy Authentifcati			
Realm			
(Leave blank if no	t required)		
User Name Password			
	💥 Cancel 📀 Ok		

We can see the test showing results.



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing 🗧 📵 🤅				
ile Options About Help				
http://192.168.1	.108:80/			
 Scan Inform 	ation $^{\circ}$ Results - List View: Dirs: 12 Files: 4 \langle Results - Tree V	/iew 🕅 Errors: 0 🔪		
Туре	Found	Response	Size	
Dir	/ www.hackingarticles.in	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: 8 Average speed: (93 requests/sec T) 901, (C) 870 requests/sec	(Select and righ	nt click for more options	

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.



	DirBuster 1.0-RC	1 - Advanced Options
HTML Parsing Options	Authentication Options	Http Options $\overline{\}$ Scan Options $\overline{\}$ DirBuster Options $\overline{\}$
File extensions to not	t process	
jpg,gif,jpeg,ico,tiff,p	ng,bmp	articl es.in
HTML elements to ex	tract links from	
F	ITML Tag	Attribute
a	-	href
img		src
form		action
script		src
iframe		src
div		
frame		src
embed		src
Tag	Attribute	
		🕂 Add
		💥 Cancel 🛛 📀 Ok

We will delete jpeg in this instance and click OK.

	DirBuster 1.0-	CI - Advanced Options	e
HTML Parsing Options	Authentication Option	s \Http Options \Scan Op	tions \DirBuster Options \
File extensions to not	process		
gif,ico,tiff,png,bmp			
	hackingarti	c les.in	
HTML elements to ex	tract links from		
Н	ITML Tag	At	tribute
a		href	
img		src	
form		action	
script		src	
iframe		src	
div		src	
frame		src	
embed		sic	
	Attributo		
lay	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	0	•	8			
File Options About	ıt Help						
Target URL (eg http://example.com:80/)							
http://testphp.vulnv	/eb.com/						
Work Method	Work Method O Use GET requests only Auto Switch (HEAD and GET)						
Number Of Threads	200 Thre 🗌 Go Faster						
Select scanning type	e: List based brute force Pure Brute Force 						
File with list of dirs/fi	les						
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt							
Char set a-zA-Z0-9%20Min length 1.S.III 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 jpeg						
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 Appli	ication Brute Forcing 🗧 🕒 🛽		
File Options About Help			
http://testphp.vulnweb.com:80/			
🕕 🕕 Scan Information \Results - List View: Dirs: 5 Files: 6 \Results - Tre	e View 🕅 🚹 Errors: 0 🔪		
Testing for dirs in / ckingarticles.in	0%		
Testing for files in / with extention .jpeg	0%		
Testing for dirs in /images/	0%		
Testing for files in /images/ with extention .jpeg	0%		
Testing for dirs in /cgi-bin/	0%		
Testing for files in /cgi-bin/ with extention .jpeg	0%		
Testing for dirs in /admin/	0% 🔲 🗖 🤟		
Current speed: 532 requests/sec (Select and right click for more opt			
Average speed: (T) 410, (C) 410 requests/sec			
Parse Queue Size: 0 Current number of running threads: 100			
Total Requests: 2050/2646589	Change		

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.

DirBuster 1.0-RC1 - Advanced Options					
/HTML Parsing Options Δ (Authentication Options Δ Http Options Δ Scan Options Δ DirBuster Options Δ					
Connection Time out Fail Case String					
30 (In Seconds)	thereIsNoWayThat-You-CanBeThere				
Limit number of requests per s	econd				
50 Number of request	s per second				
	💥 Cancel 💿 Ok				

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



DirBuster 1.0-RC1 - Advanced Options	6
/HTML Parsing Options Δ Authentication Options Δ Http Options Δ Scan Options Δ DirBuster Options	\
Connection Time out Fail Case String	
500 (In Seconds) thereIsNoWayThat-You-CanBeThere	
✓ Limit number of requests per second	
20 Number of requests per second	
www.hackingarticles.in	
🔀 Cancel 📀 Ok	

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



ile Options	About Help			
nttp://testphp	.vulnweb.com:80/	n		
🕕 Scan Info	rmation $^{\circ}$ Results - List View: Dirs: 5 Files: 11 $ angle$ Results - Tre	e View 🛝 Errors: 0 🔪		
Туре	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	
ile	/cart.php	200	196	
ile	/guestbook.php	200	196	
Dir	/AJAX/	200	196	
ile	/AJAX/index.php	200	196	
ile	/login.php	200	196	
ile	/userinfo.php	302	220	
Dir	/Mod_Rewrite_Shop/	200	196	
Dir	/hpp/	200	196	
Dir	/images/	200	154	
urrent speed	: 55 requests/sec	(Select and rig	ht click for more optio	
verage speed	l: (T) 50, (C) 53 requests/sec			
arse Queue S	ize: 0	rrent number of running	threads: 10	
Total Requests: 701/107037		Change		
		Cha	inge	
ime To Finish	: 00:33:26			
< Back	Pause Stop		Report	

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



		OV	VASP DirBuster 1.0-RC1 -	Web Application Brute Forcing	008		
File	Options A	bout Help					
http	http://testphp.vulnweb.com:80/						
	Scan Informa	ation Results -	LIST VIEW: DIRS: 4 FILES: 1 \Re	esults - Tree View \ 🔼 Errors: 0 \			
	Туре		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.pnp	h	200	196		
Curr	Current speed: 0 requests/sec (Select and right click for more options)						
Average speed: (T) 21, (C) 20 requests/sec							
Parse Queue Size: 0 Current number of running threads: 100 Total Requests: 726/2205489 Change Time To Finish: 1 Day Change			g threads: 100 hange				

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



in 😱

www.ignitetechnologies.in