

คู่มือการใช้งาน DirBuster

จัดทำโดย

1. นายพชร	พงษ์ศรี	รหัสประจำตัว	553020013-0
2. นางสาวทิฆัมพร	ฐานสมบูรณ์	รหัสประจำตัว	553020301-5
3. นางสาวพิมพ์ศิริ	ปรีดานนท์	รหัสประจำตัว	553020306-5
4. นางสาวกนิษฐา	ฤทธิแผลง	รหัสประจำตัว	553020727-1
5. นางสาวจินดารัชต์	ถมปัทม์	รหัสประจำตัว	553020730-2
6. นางสาวอนงค์นาฎ	เอี่ยมสารี	รหัสประจำตัว	553020750-6

สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสาร ชั้นปีที่ 3

อาจารย์ที่ปรึกษา ผศ.ดร. จักรชัย โสอินทร์

รายงานนี้เป็นส่วนหนึ่งของการศึกษาวิชา 322376 Information and Communication Technology Security

ภาคเรียน 1 ปีการศึกษา 2557

ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์

มหาวิทยาลัยขอนแก่น

DirBuster

DirBuster เป็นโปรแกรมภาษาจาวา ถูกออกแบบเพื่อเข้าไปยังไดเรกทอรีบน web server มีลักษณะ การทำงานคือจะเข้าไปค้นหาไดเรกทอรีต่างๆ ที่ซ่อนอยู่ใน web sever โดยที่หน้า web sever ยังมีการใช้งาน ได้เป็นปกติ

คุณสมบัติ

- มีหลาย threaded สามารถบันทึกการร้องขอได้มากกว่า 6000 การร้องขอ/วินาที
- สามารถทำงานผ่านโปรโตคอล http และ https
- สามารถค้นหาได้ทั้งไดเรกทอรีและไฟล์ข้อมูล
- สามารถค้นหาลึกเข้าไปในไดเรกทอรีที่พบ และจะค้นหาซ้ำอีกครั้งเมื่อเกิดความผิดพลาด (Error)
- สามารถดำเนินการตามรายการหรือใช้หลักการ Brute Force ค้นหาได้
- สามารถเริ่มต้นค้นหาในไดเรกทอรีใดๆ ก็ได้
- สามารถปรับเพิ่ม HTTP headers ที่ใช้งานได้
- รองรับการใช้งานพร็อกซื่
- สามารถสลับระหว่างการร้องขอแบบ HEAD และ GET ได้
- มีโหมดการวิเคราะห์และตรวจสอบเมื่อค้นหาล้มเหลวให้สามารถกลับมาเป็นค้นหาเจอได้
- สามารถใช้นามสกุลไฟล์ที่กำหนดเองได้
- สามารถปรับเปลี่ยนการดำเนินการต่างๆ ได้ในขณะที่โปรแกรมทำงานได้
- รองรับพื้นฐานสำคัญและการรับรองความถูกต้องของ NTLM
- สามารถสั่งการในระบบ GUI interface ซึ่งง่ายต่อการใช้งาน

การติดตั้งโปรแกรม DirBuster

1. ในการติดตั้งโปรแกรม DirBuster นั้นมีความสะดวก รวดเร็ว และไม่ซับซ้อน โดยเริ่มต้นให้เข้าไปทำการ download โปรแกรม DirBuster-0.12-Setup.exe จากเว็บไซต์

https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project



 ก่อนที่จะทำการติดตั้งโปรแกรม DirBuster-0.12-Setup.exe นั้น ผู้ใช้ต้องทำการตรวจสอบเครื่อง ผู้ใช้ก่อนว่ามีโปรแกรมจาวาหรือไม่ ถ้าไม่มีให้ทำการติดตั้งโปรแกรมจาวาก่อน สามารถตรวจสอบดูโปรแกรม จาวาได้ดังนี้ โดยกดปุ่ม start >> cmd แล้วพิมพ์คำว่า java -version



3. เมื่อ download เรียบร้อยแล้ว ให้ทำการติดตั้งโปรแกรม DirBuster-0.12-Setup.exe โดยกดปุ่ม

Run

Open File -	Security Warning
run this	software? Name:sers\Com\Downloads\DirBuster-0.12-Setup.exe Publisher: Unknown Publisher Type: Application
	From: C:\Users\Com\Downloads\DirBuster-0.12-Setup
V Al <u>w</u> ay	s ask before opening this file This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.

4. กดปุ่ม Browse.. เพื่อเลือกที่จัดเก็บไฟล์ที่ติดตั้ง

🕞 DirBuster Setup
Choose Install Location Choose the folder in which to install DirBuster.
Setup will install DirBuster in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.
Destination Folder C:\Users\Com\Desktop\tool\DirBuster Browse
Space required: 36.9MB Space available: 191.0GB
< <u>Back</u> <u>Next</u> > <u>Cancel</u>

5. เมื่อเลือกที่จัดเก็บไฟล์เรียบร้อยแล้ว ให้กดปุ่ม Install เพื่อติดตั้ง

Choose Start Menu Folder Choose a Start Menu folder f	r for the DirBuste	r shortcuts.		(Ventil)
Select the Start Menu folder can also enter a name to crea	in which you w ate a new folde	ould like to create r.	the program's sh	ortcuts. You
DirBuster				
7-Zip				
Accessories				
ACD Systems				
Administrative Tools				
Altova XMLSpy 2009 sp1 En	terprise Edition			
AppServ				
AppsHat				
ASUS				
ASUSDVD				
AJOJUVU				-
AVG PC TuneUp 2014				
AVG PC TuneUp 2014				
AVG PC TuneUp 2014 Do not create shortcuts Ruster Tochaller				

6. กดปุ่ม I Agree เพื่อยอมรับการติดตั้ง

🗊 DirBuster S	etup			
License Agr Please review	e ement v the license terms befor	re insta <mark>lli</mark> ng DirBuster.		
Press Page [own to see the rest of t	he agreement.		
	GNU LESSER GE Version 2.1,	ENERAL PUBLIC LICEN February 1999	NSE	<u>^</u>
Copyright (51 Franklin Everyone is of this licen	C) 1991, 1999 Free Soft Street, Fifth Floor, Bosto permitted to copy and o se document, but changi	ware Foundation, Inc on, MA 02110-1301 I distribute verbatim cop ing it is not allowed.	USA pies	
as the succ	essor of the GNU Library number 2.1.]	Public License, versio	on 2, hence	-
If you accep agreement t	t the terms of the agreen install DirBuster.	ment, dick I Agree to	continue. You must	accept the
DirBuster Instal	er		I <u>A</u> gree	Cancel

7. ดำเนินการตามขั้นตอนจนปรากฏหน้าจอ Installation Complete ซึ่งแสดงถึงการการติดตั้งโปแก รมเสร็จสมบูรณ์

G DirBuster Setup	
Installation Complete Setup was completed successfully.	
Completed	
Show <u>d</u> etails	
DirBuster Installer	
< <u>B</u> ack	se Cancel

การใช้งานโปรแกรม DirBuster

1. เปิดโปรแกรม DirBuster ที่ติดตั้งสำเร็จ

😋 🔾 🗢 📕 « Program	n Files (x86) ► DirBuster ► -	Search Dir 🔎
Organize 👻 Include	in library	:= • 🔟 🔞
☆ Favorites	Name	Date modified
Desktop	鷆 lib	12/10/2557 23:03
Downloads	apache-user-enum-1.0.txt	15/8/2551 5:05
E Recent Places	apache-user-enum-2.0.txt	15/8/2551 5:05
	DirBuster.jar	3/10/2551 15:18
🥽 Libraries	directory-list-1.0.txt	15/8/2551 5:05
Documents	directory-list-2.3-big.txt	15/8/2551 5:05
J Music	directory-list-2.3-medium.txt	15/8/2551 5:05
Pictures	directory-list-2.3-small.txt	15/8/2551 5:05
Videos	directory-list-lowercase-2.3-big.txt	15/8/2551 5:05
	directory-list-lowercase-2.3-medium.txt	15/8/2551 5:05
🖳 Computer	directory-list-lowercase-2.3-small.txt	15/8/2551 5:05
🏭 OS (C:)	ico owasp.ico	18/8/2551 21:50
DATA (D:)	🞯 Uninstall.exe	12/10/2557 23:03
Recovery (E:)		
🗣 Network		
	•	F
13 items		

2. เมื่อเปิดโปรแกรมแล้ว ให้คลิกขวาที่ DirBuster.jar แล้วเลือก Open with >> Java(TM) Platform SE binary

Organize 🔻 🛛 🔚 Oper	n 🔻 Burn	New folder	=
 ★ Favorites ■ Desktop ▶ Downloads ™ Recent Places ₩ Libraries ▶ Documents 	Name Iib apache- DirBuste direct direct	user-enum-1.0.bxt user-enum-2.0.bxt riar Open MediaInfo	Date modified 12/10/2557 23:03 15/8/2551 5:05 15/8/2551 5:05 3/10/2551 15:18
Music Pictures Videos Computer SOS (C:) DATA (D:) Recovery (F:)	direct direct direct direct direct direct direct	Convert with Rich Vide Extract files Extract Here Extract to DirBuster\ Shred with PC Faster EditPlus 3 สแกนด้วย Microsoft See Cdit with Notepad++	o Converter curity Essentials
Internet Explorer		Open with	•
Java(TM) Platform SE bir	hary	Restore previous version	ons
WinRAR archiver		Send to	•
Choose default program		Cut Copy	
		Create shortcut Delete Rename	
	•	Properties	

3. จะปรากฏหน้าโปรแกรม DirBuster ขึ้นมาดังรูป จากนั้นให้กดปุ่ม Browse เพื่อเลือกไฟล์ที่จัดเก็บ โปรแกรม DirBuster ไว้

OWASP DirBuster 0.12 - Web A	pplication Brute Forcing			
File Options About Help				
Target URL (eg http://example.co	m:80/)			
Work Method O Use GET	requests only () Auto Switch (HEA	D and GET)		
Number Of Threads	10 Thre	ads 🗌 Go Fa	ster	
Select scanning type:	List based brute force 🛛 🔿 Pure Bru	ite Force		
File with list of dirs/files				
			🔍 Browse 🕕	List Info
Char set a-zA-Z0-9%20	Min length	Max Ler	ngth 8	
Select starting options: ③ S	tandard start point 🛛 URL Fuzz			
✓ Brute Force Dirs	Be Recursive	Dir to start with	1	
Brute Force Files	Use Blank Extention	File extention	php	
URL to fuzz - /test.html?url={dir}.	asp		-	
Place complete the test details				► Start
Please complete the test details				

4. ให้เลือกไฟล์ที่จัดเก็บโปรแกรม DirBuster ไว้

Please Select	The Directory/File List You Wish To Use		x
Look In:	System32	- 🖻 🖾 🎽	
0409			
i 1033			
🗀 AdvancedI	Installers		
🗀 ar-SA			
🗀 bg-BG			
🗀 Boot			
Catroot			
Catroot2			
 ▲ 器 			•
File <u>N</u> ame:			
Files of <u>T</u> ype:	All Files		-
		Select List Ca	ancel

5. ให้คลิกเลือก directory-list-1.0.txt เพื่อแสดงข้อมูลไฟล์ออกมาที่ไดเรกทอรี แล้วกดปุ่ม Select

List

Please Sele	ct The Directory/File List You	Wish To Use
Look In:) DirBuster	- 🛍 🖄 🐸 🔡 🖿
lib apache-u apache-u DirBuster directory directory directory directory directory directory directory	user-enum-1.0.txt user-enum-2.0.txt r.jar -list-1.0.txt -list-2.3-big.txt -list-2.3-medium.txt -list-2.3-small.txt -list-lowercase-2.3-big.txt	 directory-list-lowercase-2.3-medium.txt directory-list-lowercase-2.3-small.txt owasp.ico Uninstall.exe
File <u>N</u> ame: Files of <u>T</u> ype:	directory-list-1.0.txt All Files	Select List Cancel

6. จากนั้นจะปรากฏหน้าดังรูป ให้ทำการกรอก URL ที่เราต้องการเข้าไปดูข้อมูลไฟล์ในไดเรกทอรี จากนั้นกดปุ่ม Start (ในตัวอย่างนี้เป็นเว็บไซต์ http://www.kapook.com)

S OWASP DirBuster 0.12 - Web Application Brute Forcing
File Options About Help
Target URL (eg http://example.com:80/)
www.kapook.com
Work Method O Use GET requests only (a) Auto Switch (HEAD and GET)
Number Of Threads 🖂 🖂 Go Faster
Select scanning type: List based brute force Pure Brute Force
File with list of dirs/files
C:\Program Files (x86)\DirBuster\directory-list-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 Extention File extention php
URL to fuzz - /test.html?url={dir}.asp
Please complete the test details

7. จะปรากฏไฟล์ไดเรกทอรีทั้งหมดที่มีอยู่ใน http://www.kapook.com

tp://www List View	.kapook.com:80/					
Туре	Found	Response	Size	Include	Status	
Dir Dir	/cgi-bin/	403	519	 Image: A second s	Waiting	1
lir	/new/	200	357	~	Waiting	
lir	/video/	403	517	~	Waiting	
lir	/politics/	200	356	~	Waiting	
)ir	/	200	410746	~	Scanning	
lir	/music/	200	452	~	Waiting	2000
lir	/weather/	403	519	~	Waiting	2000
lir	/images/	200	358	~	Waiting	1000
lir	/magazine/	403	520	~	Waiting	
lir	/contact/	403	519	~	Waiting	
lir	/guide/	403	517	~	Waiting	
lir	/banner/	403	518	~	Waiting	_
lir	/game/	403	516	 Image: A set of the set of the	Waiting	
urrent spe verage spe arse Queu otal Reque	ed: 0 requests/sec eed: (T) 51, (C) 51 requests/sec e Size: 0 ests: 459/3684082	c	urrent number o	(Select and of running the	right click for more o reads: 87 hange	ptior

8. ถ้าคลิกเลือกที่ Tree View จะแสดงเป็นไฟล์ folder ต่างๆ

OWASP DirBuster 0.12 - Web Application	Brute Forcing	
File Options About Help		
http://www.kapook.com:80/		
Directory Stucture	Responce Code	Responce Size
± m ² video	403	517
	200	356
ti music	200	452
	403	519
🖶 🗀 images	200	358
🖶 🗀 magazine	403	520
i contact	403	519
🖶 🖆 guide	403	517
🖶 🖓 🖾 banner	403	518
🖶 🖆 🤷 game	403	516
img ⊕	403	515
	- 202	
Current speed: /b requests/sec		(Select and right click for more options)
Average speed: (T) 27, (C) 28 requests/sec		
Parse Queue Size: 0		Current number of running threads: 87
Total Requests: 6849/13035971		Change
Time To Finish: 5 Days		
Back DD Pause	□ Stop	Report
Brute forceing dirs in /		/883/

9. สามารถเลือกไฟล์ที่เราต้องการดูข้อมูลได้

OWASP DirBuster 0.12 - Web Application	Brute Forcing		
File Options About Help			
http://www.kapook.com;80/			
List View Tree View	T		
Directory Stucture	Responce	Code Responce Size	2
🕀 🧰 kapook_2014	403	523	_
🕀 🧀 images_CF	403	521	
🕀 🗀 sitemap	200	356	
🖶 🖆 ads	403	515	222
🥭 admin	401	745	
⊕ ⊡ show	403	516	
profile	403	519	
🖽 🞑 google	200	449	
event	403	51/	
	403	520	
wallpaper	200	35/	-
Current speed: 502 requests/sec		(Select and right clic	k for more options)
Average speed: (T) 117, (C) 492 requests/sec			
Parse Queue Size: 0		Current number of running threads: 87	
Total Requests: 54240/22954621			
Time To Finish: 12:55:45			
Back D Pause	□ Stop	[🗐 Report
Brute forceing dirs in /			/HorizBar_12/

10. ถ้าต้องการดูข้อมูลของไฟล์นั้นๆ ให้ทำการคลิกขวาที่ไฟล์แล้วเลือก View Response ก็จะแสดง ข้อมูลต่างๆ ของไดเรกทอรีนั้นๆ

OWASP DirBuster 0.12 - Web Application E	Brute Forcing		
File Options About Help			
http://www.kapook.com:80/			
Directory Stucture	Response Code		Responce Size
kapack 2014	402		
	403		521
the citeman	200	-	256
the mining and s	403		515
	401		745
💼 🗀 🚮 🕥 Open In Browser	403		516
🕀 🧀 pr View Response	403		519
🕀 🗁 99 🗊 Copy UBI	200	4	149
event	403	1	517
includes	403	1	520
🖶 🗀 wallpaper	200	3	357 👻
Current speed: 507 requests/sec			(Select and right click for more options)
Average speed: (T) 194, (C) 476 requests/sec			
Parse Oueue Size: 0		Current pu	umber of running threads 97
Total Requests: 112565/31172931		Current nu	
			Change
Time To Finish: 18:07:32			
Back II Pause	□ Stop		Report
Brute forceing dirs in /			/fly4/

11. เมื่อกดเลือก View Response แล้วจะปรากฏข้อมูลดังรูป

DirBuster 0.12 View Response
Responce for HTTP/1.0 401 UnauthorizedServer: nginx/1.4.4Date: Thu, 16 Oct 2014 23:19:38 GMTContent-Type: text/htm
Raw Response \ Base Case Information \ Raw Response vs Base Case \ Diff Raw vs Base \
HTTP/1.0 401 Unauthorized
Date: Thu, 16 Oct 2014 23:19:38 GMT
Content-Type: text/html; charset=iso-8859-1 Content-Length: 401
WWW-Authenticate: Basic realm="Password Required" X-Cache: MISS from cache125
X-Cache-Lookup: MISS from cache125:3128
Via: 1.0 cache125 (squid/3.1.20) Connection: keep-alive
HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"
<ntml><nead><title>401 Authorization Required</title></nead></ntml>
<body> <h1>Authorization Required</h1></body>
This server could not verify that you are suffered to see the degument.
requested. Either you supplied the wrong
credentials (e.g., bad password), or your browser doesn't understand how to supply
the credentials required.
X Close

Note : กรณีที่ค้นหาแล้วพบไดเรกทอรี่ /phpmyadmin/ ถ้าทราบ username และ password ก็สามารถ เข้าไปดูข้อมูลในฐานข้อมูลนั้นได้ แต่ถ้าไม่ทราบก็ไม่สามารถเข้าดูข้อมูลในฐานข้อมูลนั้นได้เช่นกัน และในกรณี ที่ค้นหาแล้วพบไดเรกทอรี่ /phpmyadmin/ ถ้าฐานข้อมูลนั้นไม่ได้ตั้งค่า username และ password ไว้ก็ สามารถเข้าไปดูข้อมูลในฐานข้อมูลนั้นได้เลย

(
l	() () () () () () () () () ()	🏟 🟠 🛠 🗄
1	File Edit View Favorites Tools Help	
3	X P Search INBOXAGE ************************************	🛞 More 🎗
- BURN BURN ENGL	Windows Security The server www.gunthestar.com at phpMyAdmin localhost requires a username and password. Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection). Image: User name Password Remember my credentials OK	
r		

12. ในส่วนของ Dir to start with เป็นการค้นหาไดเรกทอรีเฉพาะที่เราต้องการค้นหา โดยนำชื่อ ไดเรกทอรีที่เราต้องการค้นหามากรอกใส่ในช่องนี้ได้เลย จากนั้นกดปุ่ม Start เพื่อค้นหาไดเรกทอรีที่เรา ต้องการ (ตัวอย่างเช่น ต้องการที่จะค้นหาไดเรกทอรีที่มีชื่อว่า /images/)

OWASP DirBuster 0.12 - Web App	lication Brute Forcing		
File Options About Help			
Target URL (eg http://example.com:80/)		
http://www.kapook.com			
Work Method Ouse GET reque	ests only () Auto Switch (HEAD and	GET)	
Number Of Threads	10 Threade	s 🔄 Go Faste	r
Select scanning type: List t File with list of dirs/files 	ased brute force OPure Brute Fo	orce	
C:\Program Files (x86)\DirBuster\direct	pry-list-1.0.txt		🔍 Browse 🕕 List Info
Char set a-zA-Z0-9%20	▼ Min length 1	Max Length	8
Select starting options: Standa 	ard start point 🔿 URL Fuzz		
Brute Force Dirs	Be Recursive	Dir to start with	/images/
Brute Force Files	Use Blank Extention	File extention	php
URL to fuzz - /test.html?url={dir}.asp			
/			
Exit			Start
DirBuster Stopped			/images/GMA/

13. โปรแกรมจะทำการค้นหาไฟล์ที่เกี่ยวข้องกับไดเรกทอรีที่ชื่อว่า /images/ ดังรูป

Found ges/ ges/pr/ ges/music/ i // //msn_plus.php //msn_plus.php paper ert ook-loggo-file	Response 200 403 403 200 301 301 301	Size 292107 520 523 321 630 431 69 448 642 636	Include	Status Scanning Waiting Waiting Waiting Waiting Return code for first
ges/ ges/pr/ ges/music/ i/ i/msn_plus.php i/msn_plus.php paper ert gaper ert	200 403 403 200 301 302 200 301 301 301	292107 520 523 321 630 431 69 448 642 636	> > > >	Scanning Waiting Waiting Waiting Return code for first
ges/pr/ ges/music/ i/ i/msn_plus.php /msn_plus.php paper ert gaper ert	403 403 200 301 302 200 301 301 301	520 523 321 630 431 69 448 642 636		Waiting Waiting Waiting Return code for first
ges/music/ // //msn_plus.php /msn_plus.php paper ert ert ook-logo-file	403 200 301 302 200 301 301 301	523 321 630 431 69 448 642 636		Waiting Waiting Waiting Return code for first
i //msn_plus.php /msn_plus.php paper ert ook-logo-file	200 301 302 200 301 301 301	321 630 431 69 448 642 636		Waiting Waiting Return code for first
i // //msn_plus.php /msn_plus.php paper ert ert ook-logo-file	301 302 200 301 301 301	630 431 69 448 642 636		Waiting Return code for first
// //msn_plus.php paper ert ook-logo-file	302 200 301 301 301	431 69 448 642 636		Waiting Return code for first
//msn_plus.php //msn_plus.php paper ert ook-logo-file	200 301 301 301	69 448 642 636		Return code for first
/msn_plus.php paper ert ook-logo-file	200 301 301 301	448 642 636		
paper ert ook-logo-file	301 301 301	642 636		
ert ook-logo-file	301 301	636		
ook-logo-file	301			
		656		
sx.pnp	200	321		
tics/	200	388	~	Waiting
ert/	200	388	 Image: A set of the set of the	Waiting
equests/sec) 10, (C) 0 requests/sec			(Select an	nd right click for more opti
0	Cur	rrent number of rur	nning threads	s: 10
4/1983787			Cha	ange
	equests/sec) 10, (C) 0 requests/sec 0 74/1983787 III Pause Sto	equests/sec -) 10, (C) 0 requests/sec 0 Cu -/4/1963787	equests/sec) 10, (C) 0 requests/sec 0 Current number of rur /4/1963787	equests/sec (Select ar 1) 10, (C) 0 requests/sec 0 Current number of running threads 14/1963787

14. ตัวอย่างการค้นหาไฟล์ในไดเรกทอรีของ http://10.199.7.51:80/ และเลือก /phpmyadmin/ ในไดเรกทอรีที่เป็นฐานข้อมูล

OWASP D	DirBuster 0.12 - Web Application Brute Forcing						
File Optic	ons About Help						
http://10.19	9.7.51:80/						
List View	Tree View						
Туре	Found	Response	Size	Include	Status		
Dir	/security/img/	403	259	×	Waiting		
File	/security/lang.php	200	182				
File	/security/xampp.js	200	839				
Dir	/examples/	503	270	~	Waiting		
Dir	/licenses/	200	179	~	Waiting		
Dir	/error/	403	269	~	Waiting		
Dir	/%20/	403	269	~	Waiting		
Dir	/restricted/	200	571	~	Waiting		
Dir	/*checkout*/	403	269	~	Waiting		
Dir	/phpmyadmin/	200	997	~	Waiting		
Dir	/webalizer/	200	4151	×	Waiting		
Dir	/*docroot*/	403	269	~	Waiting		
File	/webalizer/usage_201409.html	200	95021		•		
Current spe Average spe	eed: 1550 requests/sec eed: (T) 671, (C) 1386 requests/sec			(Select and	right click for more options;		
Parse Queu	e Size: 0		Current number o	f running th	reads: 99		
Total Reque	ects: 57723/3755045						
. etai nequi			99		hange		
Time To Fir	nish: 00:44:27						
Ba	ack 00 Pause Stop				Report		
Brute forcei	ng dirs in /				/debat		

15. จากนั้นจะปรากฏหน้าของฐานข้อมูลที่ได้จากการเลือกไดเรกทอรี /phpmyadmin/

KKU Internet Access Auth × F F	acebook × 🕅 Boot	itrap WorkShop ?db=webtech&	× 🎊 10.199.7	.51 / 127.0.0.1 / w	ve ×	=550	le90a5a00k	0810c63c45cd99fd1a7a5		
phpMuAdmin	🔶 📑 ເໝີຣ໌ຟເວລຣ໌: 127.0.0.1 » 🗃 ຊູ	ນນ້ອນຸລ: webtech	» 🔝 ดาราง: persor	1						
	🔲 เปิดดู 📝 โครงสร้าง 🔒	🕽 SQL 🔍 ค่	ันหา 👫 แทรศ	ก 🔜 ส่งออเ	ก 📑 นำเข้า		สิทธิ 🥜	กระบวนการ 💿 การติดตา	ม 🕮 ทริกเกอร์	
(คารางล่าสด) •	+ ตัวเลือก		_							
	← – – → – – – – –	Uid User	Pwd	FName	LName	Sex	Tel	Email		
The state of the s	🔲 🥜 แก้ไข 🚽 ี่ คัดลอก 🥥 ลบ	1 psk	1234	SMJ	PSK	М	258258	smj#kkhhf Click to mark	er lunmark	
information_schema	🗌 🥜 แก้ไข 🚮 🕯 คัดลอก 🥥 ลบ	2 ixuou	123456	Songvut	Butham	М	0843928845	ixuou@ixuou.com	b copy column name	
🖶 🕞 mysql	🔲 🥜 แก้ไข 🚮 🕯 คัดลอก 😂 ลบ	3 htz	k010437	kan	kanchanok	f	080 080 08	tanniiz.i.vip@gmail.com		
+- performance_schema	🗌 🥜 ແກ້ໃນ 👫 คัดลอก 🤤 ລນ	4 kritanon	123456	kritanon	Sangchompoo	m	0883342133	Bm_hi-school@hotmail.com		
test	🔲 🥜 แก้ไข 👫 คัดลอก 🤤 ลบ	5 xeer	xeer	krisana	pimpanit	m	0966742680	killazaold1993@gmail.com		
+ webauth	🗌 🥔 แก้ไข 👫 ตัดลอก 🥥 ลบ	6 Constantum	816214	kittinut	private	m	0831298728	kittinut_p@kkumail.com		
- webtech	🗌 🥒 แก้ไข 👫 ่ คัดลอก 🔾 ลบ	7 kanok	123456789	kanokporn	martkaew	f	0800000000	kanok@gmail.com		
	🗌 🥔 แก้ไข 🖟 ่ คัดลอก 🥥 ลบ	8 poohpan	4558363	Apichit	Tischob	m	0876768282	poohpanbakery@live.com		
😐 🎤 person	🗌 🥒 แก้ไข 🖟 ่ คัดลอก 🔘 ลบ	9 jane	242536	Chenchira	Thabphuta	F	0832868024	janejajane24@hotmail.co.th		
	🗌 🥒 แก้ไข 🖟 ้คัดลอก 🙆 ลบ	10 Gubenzza	123456789	Piyawat	Namwanta	М	0833333333	Gubenzza@hotmail.co.uk		
	🗌 🥒 แก้ไข 🖫 ่ คัดลอก 🙆 ลบ	11 Jeab	0833568037	Tatiya	Ouakan	F	0922658037	TATIYA@hotmail.com		
	🗆 🥒 แก้ไข 🖫 ตัดลอก 🙆 ลบ	12 axeger001	12345	phuwanai	puangmalai	М	1234567890	axeger001@hotmail.com		
	🗆 🥒 แก้ไข 🚟 คัดลอก 🙆 ลบ	13 wasitaaa	1409901044990	wasita	votachai	f	0823017415	wasitaaa 9999@hotmail.com		
	🗆 🥒 แก้ไข 🚟 คัดลอก 🥥 ลบ	14 kanokpo	123456	kanok	zxcybbn	f	0800000000	ka@gmail.com		
	🗌 🥒 ແກ້ໃນ 🖼 ຄົດລວກ 🔘 ລາ	15 Pongpang	2112	Napaporn	Jinsawaeng	F	0831415691	pang 9989@hotmail.com		
	🗆 🥜 แก้ไข 😼 คัดลอก 🛆 ลบ	16 Warapom	02112536	Waraporn	Neatprom	F	0801956808	arliweiw@hotmail.com		
	🗌 🥒 แก้ไข 👫 คัดออก 🖨 อบ	17 ing	291036	ketsuda	pholnamin	f	0812558377	ketsudaaing@gmail.com		
	🗆 🥜 แก้ไข 🖫 คัดออก 🖨 อบ	18 numm	num9999999999	kliawpan	ledsanchai	f	0000000000	mani u47341@gmail.com		
	🗌 🥒 แก้ไข 🖫 ตัดออก 🦰 อน	19 akrapol	1234	akrapol	akrapol	m	1234	ak@gmail.com		
	🔾 🥜 ແກ້ເມ 🦉 ທີ່ທີ່ແມ່ກ 🥥 ແມ	20 maewmile	123/56789	maowmiio	memy	F	0821234567	memy/090909@gmail.com		
		21 TARLONY	12345	DATCHANON	CAHOROOBUT	1	111111	mail		
		22 Iloungpingli	12345	Nadaana	Tonongnan	F	0904116733	onk kno 01@hotmail.com		
		22 inputigpingin	123430	Narong	Rodoo	M	0004115755	spk_kps_on@notimali.com		
	📄 🖉 แก่เว 📲 ผดสอก 🥥 สบ	2.5 toun2	12.34	ivalong	Donee	ivi	00344499999	stacii2@notriall.com		

16. ตัวอย่างการค้นหาไฟล์ในไดเรกทอรีของ http://www.kku.ac.th จากนั้นกดปุ่ม Start

OWASP DirBuster 0.12 - Web Application Brute Forcing
File Options About Help
Target URL (eg http://example.com:80/)
http://www.kku.ac.th
Work Method Ouse GET requests only (a) Auto Switch (HEAD and GET)
Number Of Threads 99 Threads Go Faster
Select scanning type: List based brute force Pure Brute Force
File with list of dirs/files
C:\Users\BiGz\Desktop\DirBuster-0.12\DirBuster-0.12\directory-list-lowercase-2.3-small.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 /php
✓ Brute Force Files Use Blank Extention File extention html
URL to fuzz - /test.html?url={dir}.asp
/
Start DirBuster Stopped

17. จะปรากฏไฟล์ทั้งหมดที่ค้นหาจาก http://www.kku.ac.th จากนั้นกดเลือกที่ไฟล์ /usage/usage_201301.html เพื่อเรียกดูข้อมูลของไฟล์

tp://www List View	.kku.ac.th:80/ \ Tree View \				
Туре	Found	Response	Size	Include	Status
)ir	/kkuchannel/	200	202	×	Waiting
)ir	/contact/	200	339	~	Waiting
)ir	/kkuchannel/jwplayer/	403	495	~	Waiting
ile	/kkuchannel/jwplayer/check.php	200	835		
)ir	/bus/	200	3313	~	Waiting
ile	/future/kkufuture01.pdf	200	231122		
)ir	/rs/	200	362	~	Waiting
)ir	/vpn/vpn_files/	403	489	~	Waiting
)ir	/president/	200	1362	~	Waiting
ile	/usage/usage_201301.html	200	37581		
ile	/usage/usage_201212.html	200	166923		
ile	/usage/usage_201211.html	200	165939		
)ir	/branding/logo/	403	489	~	Waiting
urrent spe verage spe arse Queue	ed: 470 requests/sec eed: (T) 473, (C) 273 requests/sec e Size: 0	C	urrent number o	(Select and of running th	right click for more option reads: 99
	etc: 11842/19428444	9	9	C	hange

18. เมื่อกดเลือกที่ไฟล์ /usage/usage 201301.html แล้ว จะปรากฏข้อมูลดังรูป

KKU Internet Access Auth: × 🖪 (2) 322376 Security	🗴 🐨 🕷 สังกันระบบสำหภุณาการรมกาย ทะ 🗴 🚺 BootStrap WorkShop	× 10.199.7.51 /	127.0.01 / ws	🗴 🍐 Usage Statistics for www.i 🔺 🔪	
← → C www.kku.ac.th/usage/usage_200	1301.html				☆ =
Usage Statistics for www.kku.ac.	th				1
Summary Period: January 2013					
Generated 27-Jan-2013 00:15 ICT					
	[Daily Statistics] [Hously Statistics] [URLs] [Entry] [Exit] [Sites	[Referren] [Search] [Ag	anta] [Countrie	al	
	Monthly Statistics for Janu	ary 2013			
	Total Hits		6857		
	Total Files		4564		
	Total Pages		6386		
	Total Visits		9		
	Total KBytes		2275		
	Total Unique Sites		2		
	Total Unique URLs		1		
	Total Unique Referrers		1		
	Total Unique User Agents		2		
		Avg	Max		
	Hits per Hour	142	2446		
	Hits per Day	3428	4781		
	Files per Day	2282	2488		
	Pages per Day	3193	4310		
	Sites per Day	1	2		
	Visits per Day	4	6		
	KBytes per Day	1138	2275		
	Hits by Response Code	Hits by Response Code			
	Code 200 - OK	66.56%	4564		
	Code 403 - Forbidden	33.44%	2293		
	B				

สรุป

ในบทเรียนนี้ได้อธิบายถึงวิธีการติดตั้งและการใช้งานของโปรแกรม DirBuster ซึ่งเป็นโปรแกรมที่ใช้ ค้นหาไดเรกทอรีต่างๆ ที่ซ่อนอยู่ใน web sever นอกจากนี้ยังมีตัวอย่างการใช้งานโปรแกรม DirBuster อีกด้วย **เอกสารอ้างอิง**

1. DirBuster คือ. ค้นเมื่อ 15 ตุลาคม 2557, จาก

http://roshanhackstudy.blogspot.com/2011/05/website-directory-scanner.html

- DirBuster. ค้นเมื่อ 15 ตุลาคม 2557, จาก https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
- หลักการทำงาน DirBuster. ค้นเมื่อ 15 ตุลาคม 2557, จาก http://www.youtube.com/watch?v=aHCeG4-0olM