



คู่มือการใช้งาน

DirBuster

จัดทำโดย

1. นายเพชร	พงษ์ศรี	รหัสประจำตัว	553020013-0
2. นางสาวทิฆัมพร	ฐานสมบุรณ์	รหัสประจำตัว	553020301-5
3. นางสาวพิมพ์ศิริ	ปรีदानนท์	รหัสประจำตัว	553020306-5
4. นางสาวกนิษฐา	ฤทธิผล	รหัสประจำตัว	553020727-1
5. นางสาวจินดารัตน์	ถนบัทม์	รหัสประจำตัว	553020730-2
6. นางสาวอนงค์นาฏ	เอี่ยมสารี	รหัสประจำตัว	553020750-6

สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสาร ชั้นปีที่ 3

อาจารย์ที่ปรึกษา

ผศ.ดร. จักรชัย ไสอินทร์

รายงานนี้เป็นส่วนหนึ่งของการศึกษาวิชา 322376 Information and Communication Technology Security

ภาคเรียน 1 ปีการศึกษา 2557

ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์

มหาวิทยาลัยขอนแก่น

DirBuster

DirBuster เป็นโปรแกรมภาษาจาวา ถูกออกแบบเพื่อเข้าไปยังไดเรกทอรีบน web server มีลักษณะการทำงานคือจะเข้าไปค้นหาไดเรกทอรีต่างๆ ที่ซ่อนอยู่ใน web sever โดยที่หน้า web sever ยังมีการใช้งานได้เป็นปกติ

คุณสมบัติ

- มีหลาย threaded สามารถบันทึกการร้องขอได้มากกว่า 6000 การร้องขอ/วินาที
- สามารถทำงานผ่านโปรโตคอล http และ https
- สามารถค้นหาได้ทั้งไดเรกทอรีและไฟล์ข้อมูล
- สามารถค้นหาหลักเข้าไปในไดเรกทอรีที่พบ และจะค้นหาซ้ำอีกครั้งเมื่อเกิดความผิดพลาด (Error)
- สามารถดำเนินการตามรายการหรือใช้หลักการ Brute Force ค้นหาได้
- สามารถเริ่มต้นค้นหาในไดเรกทอรีใดๆ ก็ได้
- สามารถปรับเพิ่ม HTTP headers ที่ใช้งานได้
- รองรับการใช้งานพรีออกซี
- 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

Category:OWASP DirBuster Project

This historical page is now part of the OWASP archive.
 This page contains content that is outdated and is no longer being maintained. It is provided as a courtesy for individuals who are still using these technologies. This page may contain URLs that were once valid but may now link to sites or pages that no longer exist.
 Please use the newer Edition(s) like OWASP Zed Attack Proxy Project

OWASP PROJECTS
 INACTIVE OWASP PROJECT

DirBuster is a multi threaded java application designed to brute force directories and files names on web/application servers. Often is the case now of what looks like a web server in a state of default installation is actually not, and has pages and applications hidden within. DirBuster attempts to find these.

However tools of this nature are often as only good as the directory and file list they come with. A different approach was taken to generating this. The list was generated from scratch, by crawling the Internet and collecting the directory and files that are actually used by developers! DirBuster comes a total of 9 different lists (Further information can be found below), this makes DirBuster extremely effective at finding those hidden files and directories. And if that was not enough DirBuster also has the option to perform a pure brute force, which leaves the hidden directories and files nowhere to hide! If you have the time .)

DirBuster Fork
 Please note that DirBuster is currently an inactive project.

2. ก่อนที่จะทำการติดตั้งโปรแกรม DirBuster-0.12-Setup.exe นั้น ผู้ใช้ต้องทำการตรวจสอบเครื่องผู้ใช้อีก่อนว่ามีโปรแกรมจาวาหรือไม่ ถ้าไม่มีให้ทำการติดตั้งโปรแกรมจาวาก่อน สามารถตรวจสอบดูโปรแกรมจาวาได้ดังนี้ โดยกดปุ่ม start >> cmd แล้วพิมพ์คำว่า java -version

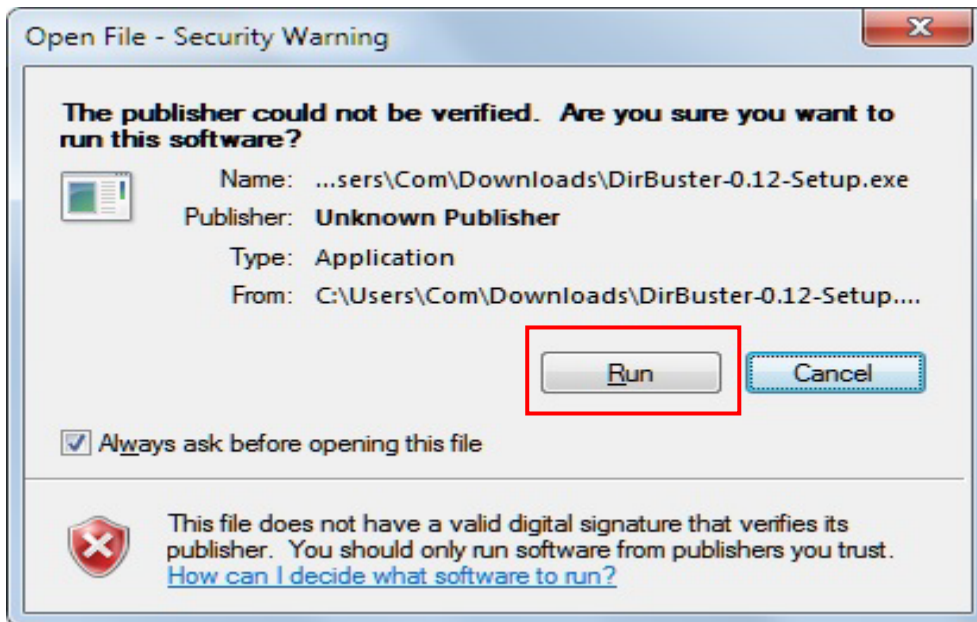
```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

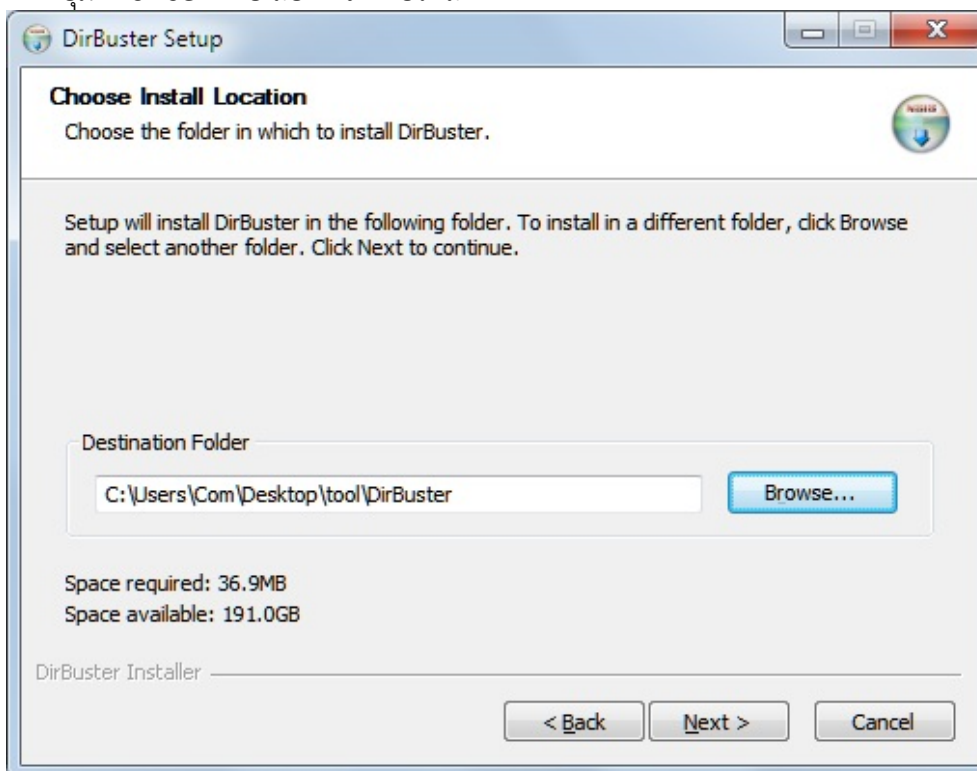
C:\Users\Com>java -version
java version "1.7.0_09"
Java(TM) SE Runtime Environment (build 1.7.0_09-b05)
Java HotSpot(TM) 64-Bit Server VM (build 23.5-b02, mixed mode)

C:\Users\Com>
  
```

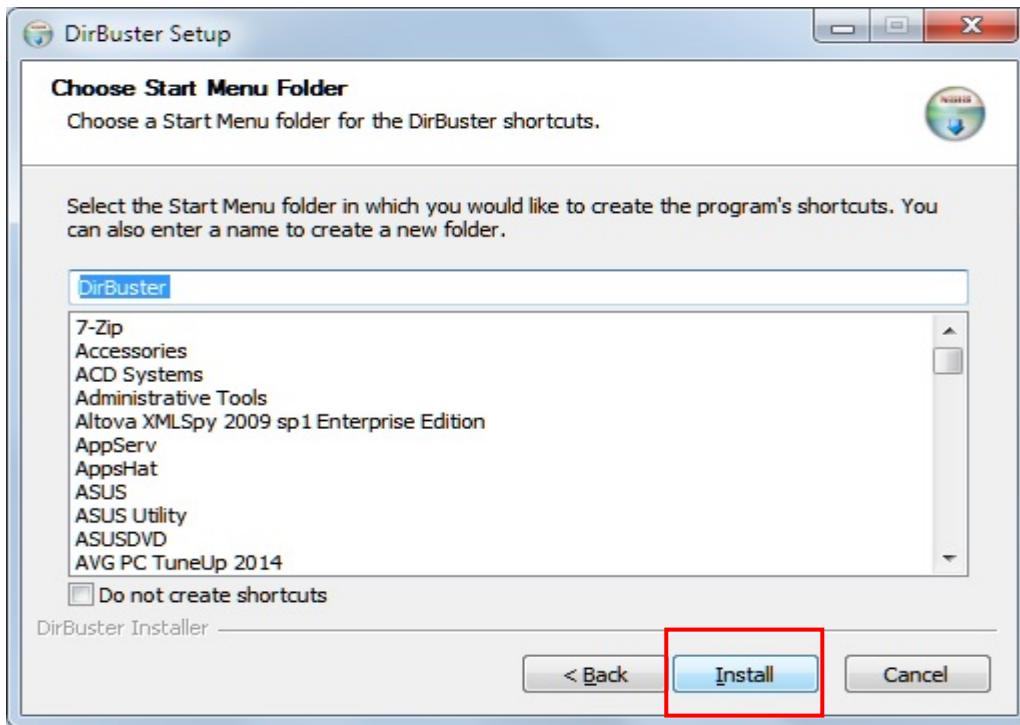
3. เมื่อ download เรียบร้อยแล้ว ให้ทำการติดตั้งโปรแกรม DirBuster-0.12-Setup.exe โดยกดปุ่ม Run



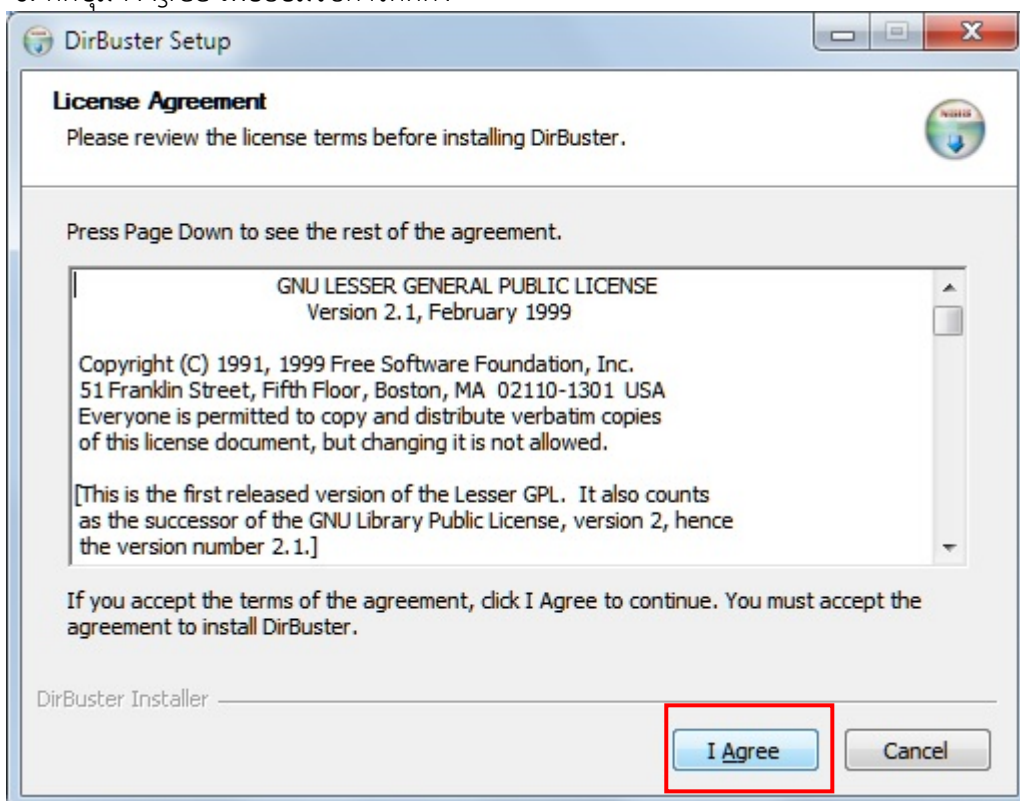
4. กดปุ่ม Browse.. เพื่อเลือกที่จัดเก็บไฟล์ที่ติดตั้ง



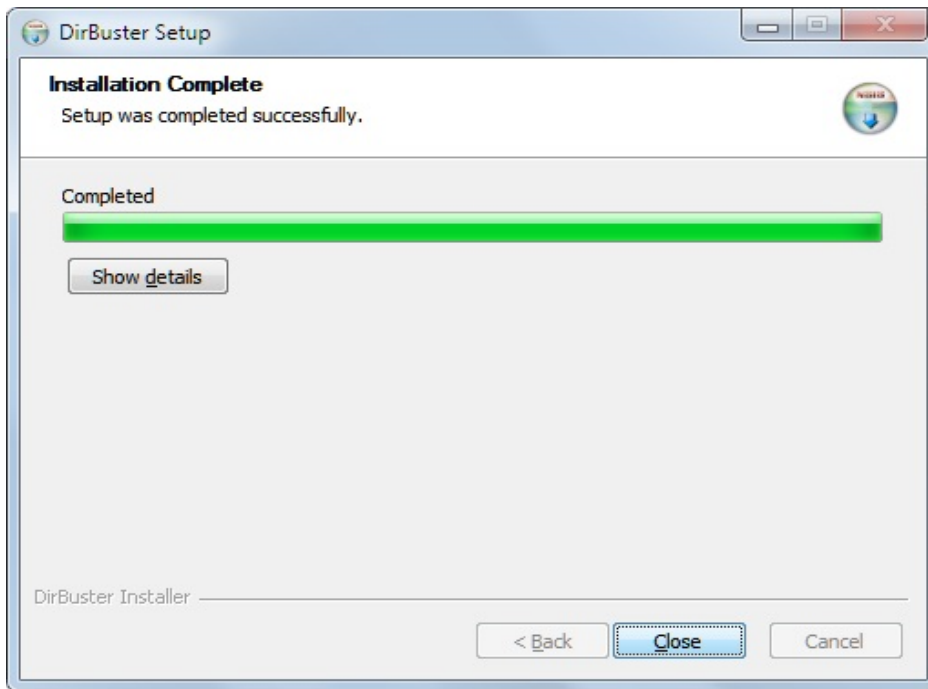
5. เมื่อเลือกที่จัดเก็บไฟล์เรียบร้อยแล้ว ให้กดปุ่ม Install เพื่อติดตั้ง



6. กดปุ่ม I Agree เพื่อยอมรับการติดตั้ง

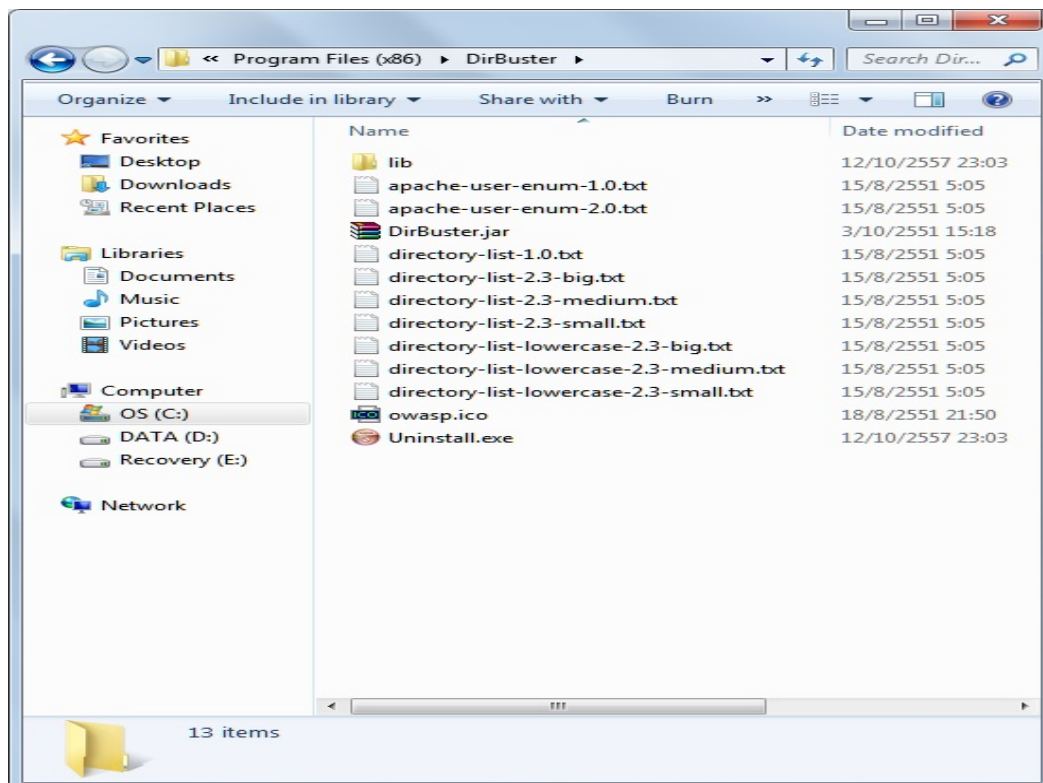


7. ดำเนินการตามขั้นตอนจนปรากฏหน้าจอ Installation Complete ซึ่งแสดงถึงการการติดตั้งโปรแกรมเสร็จสมบูรณ์

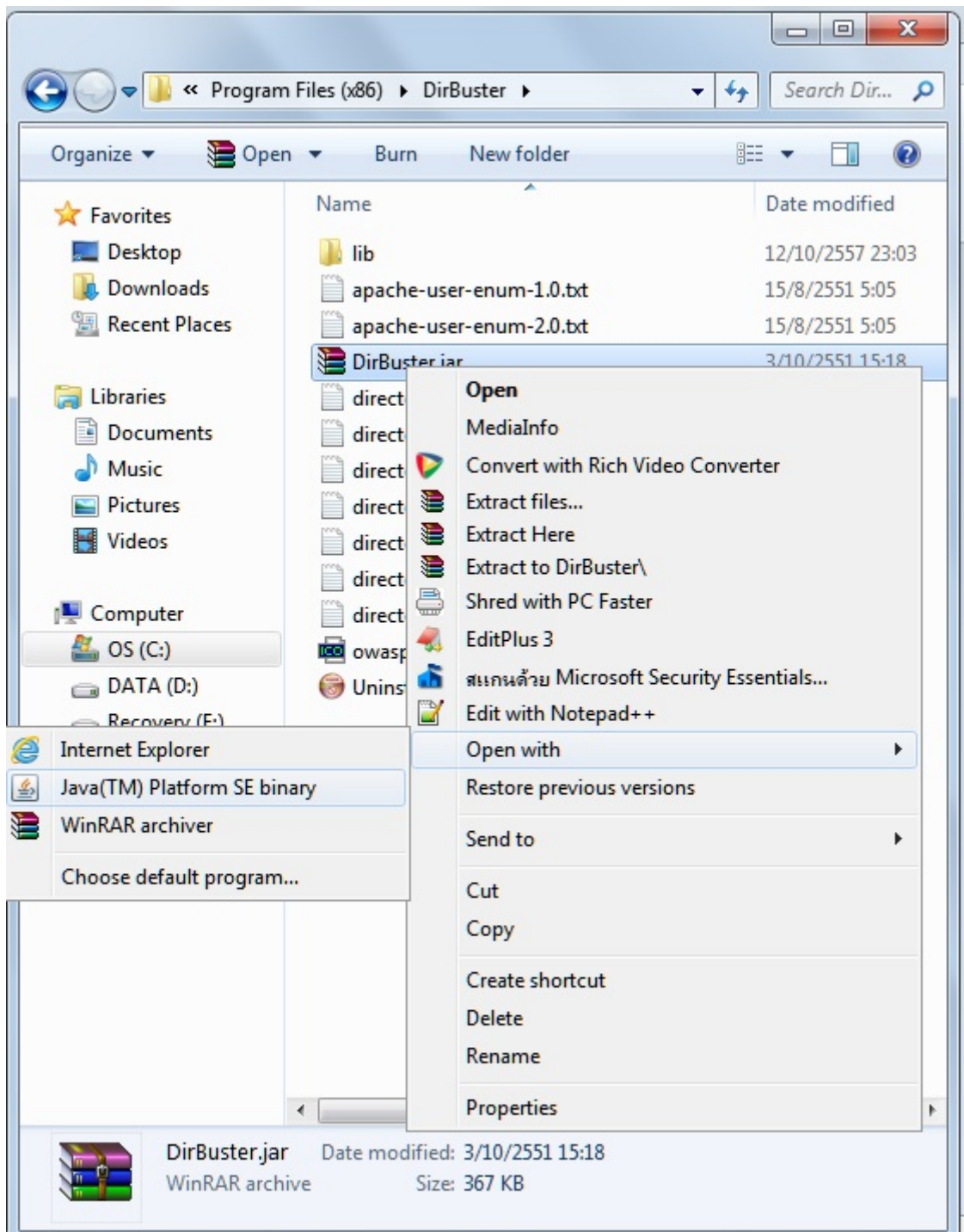


- การใช้งานโปรแกรม DirBuster

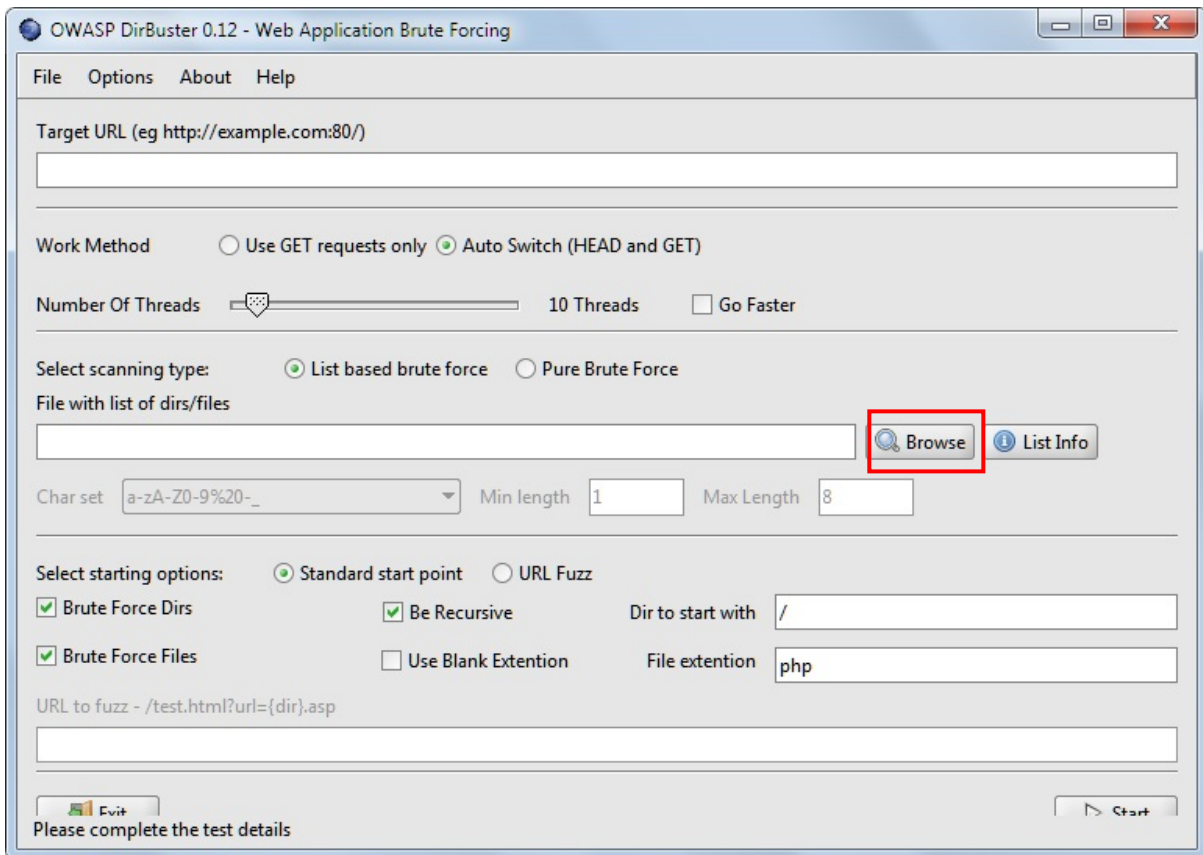
1. เปิดโปรแกรม DirBuster ที่ติดตั้งสำเร็จ



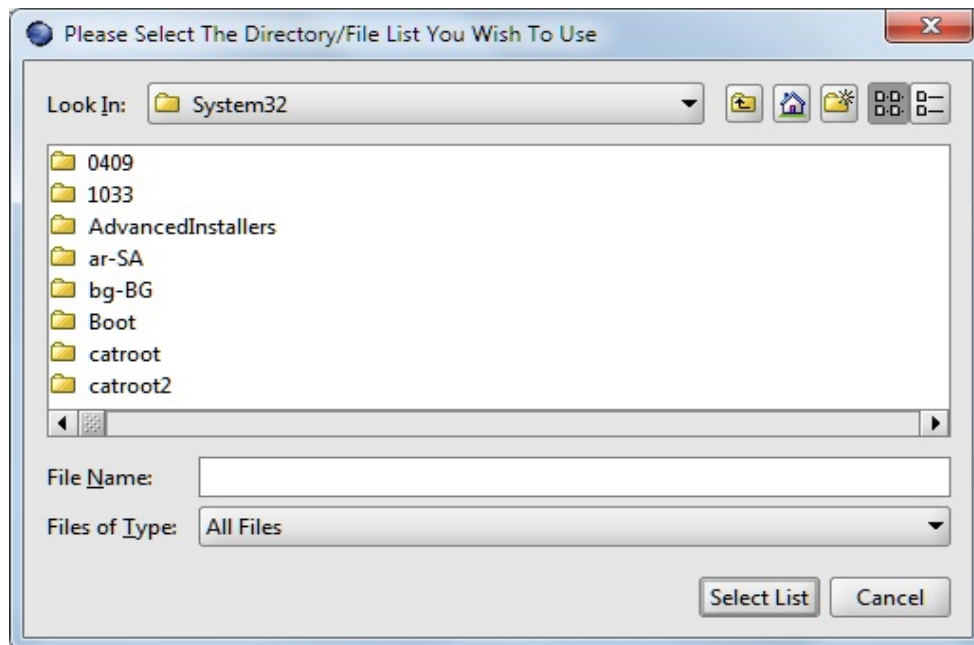
2. เมื่อเปิดโปรแกรมแล้ว ให้คลิกขวาที่ DirBuster.jar แล้วเลือก Open with >> Java(TM) Platform SE binary



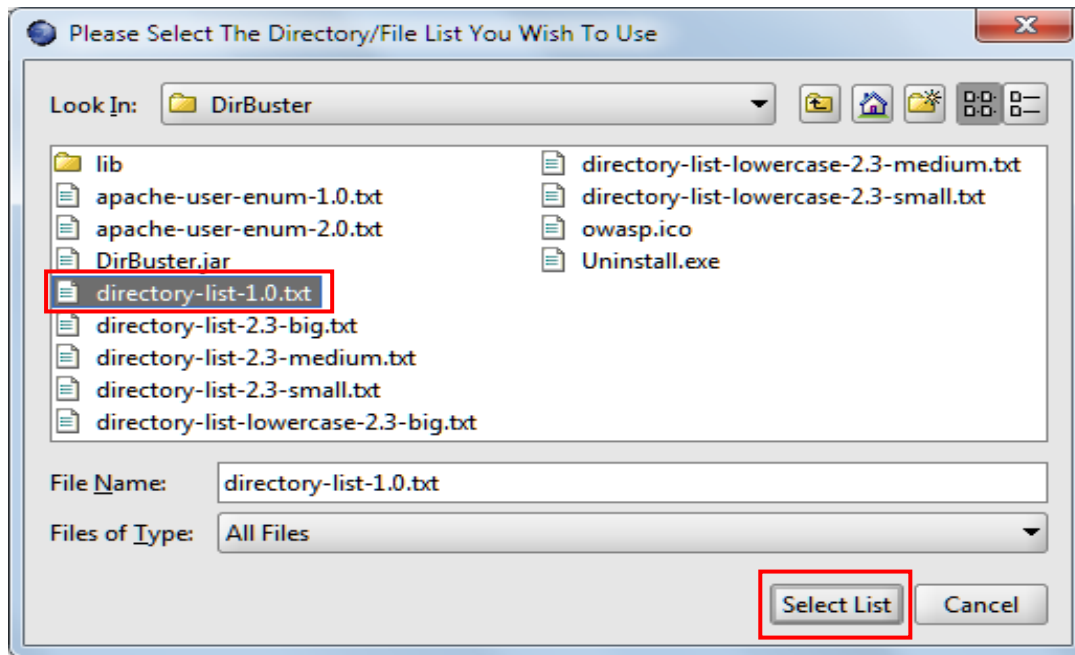
3. จะปรากฏหน้าโปรแกรม DirBuster ขึ้นมาดังรูป จากนั้นให้กดปุ่ม Browse เพื่อเลือกไฟล์ที่จัดเก็บโปรแกรม DirBuster ได้



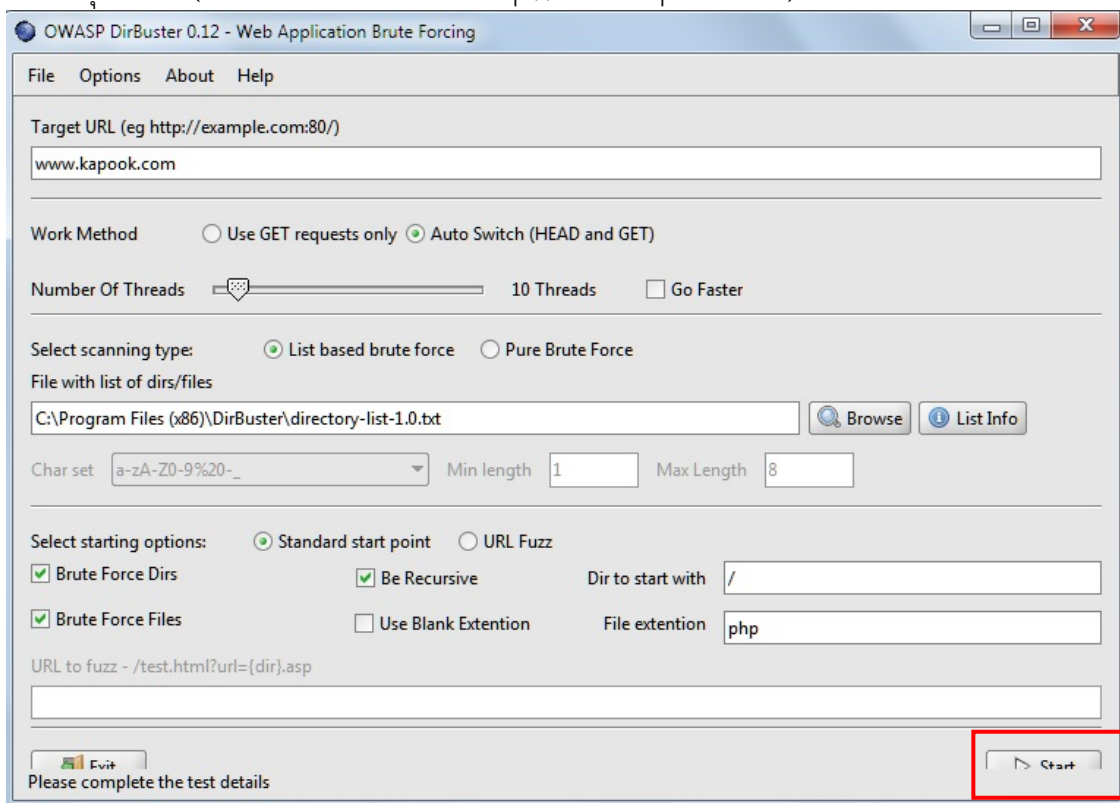
4. ให้เลือกไฟล์ที่จัดเก็บโปรแกรม DirBuster ไว้



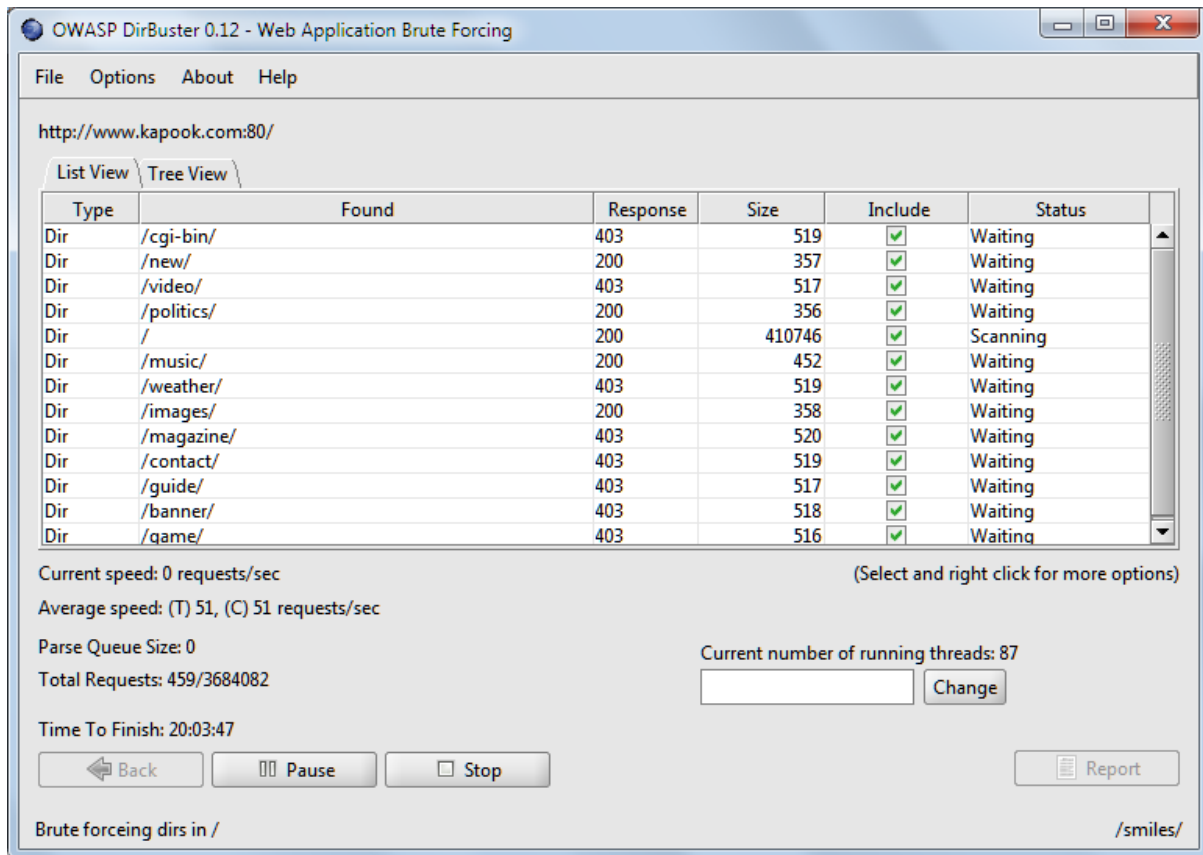
5. ให้คลิกเลือก directory-list-1.0.txt เพื่อแสดงข้อมูลไฟล์ออกมาที่ไดเรกทอรี แล้วกดปุ่ม Select List



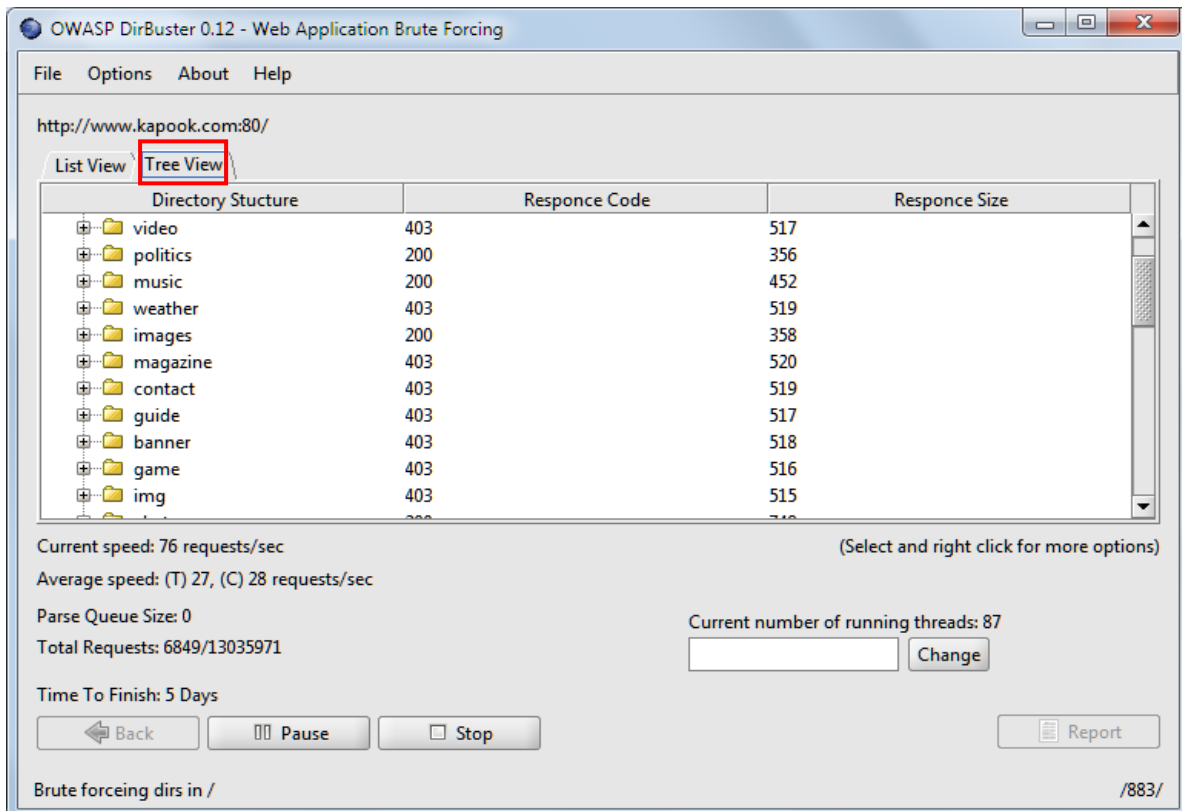
6. จากนั้นจะปรากฏหน้าต่างรูป ให้ทำการกรอก URL ที่เราต้องการเข้าไปดูข้อมูลไฟล์ในโดเมนหรือจากนั้นกดปุ่ม Start (ในตัวอย่างนี้เป็นเว็บไซต์ <http://www.kapook.com>)



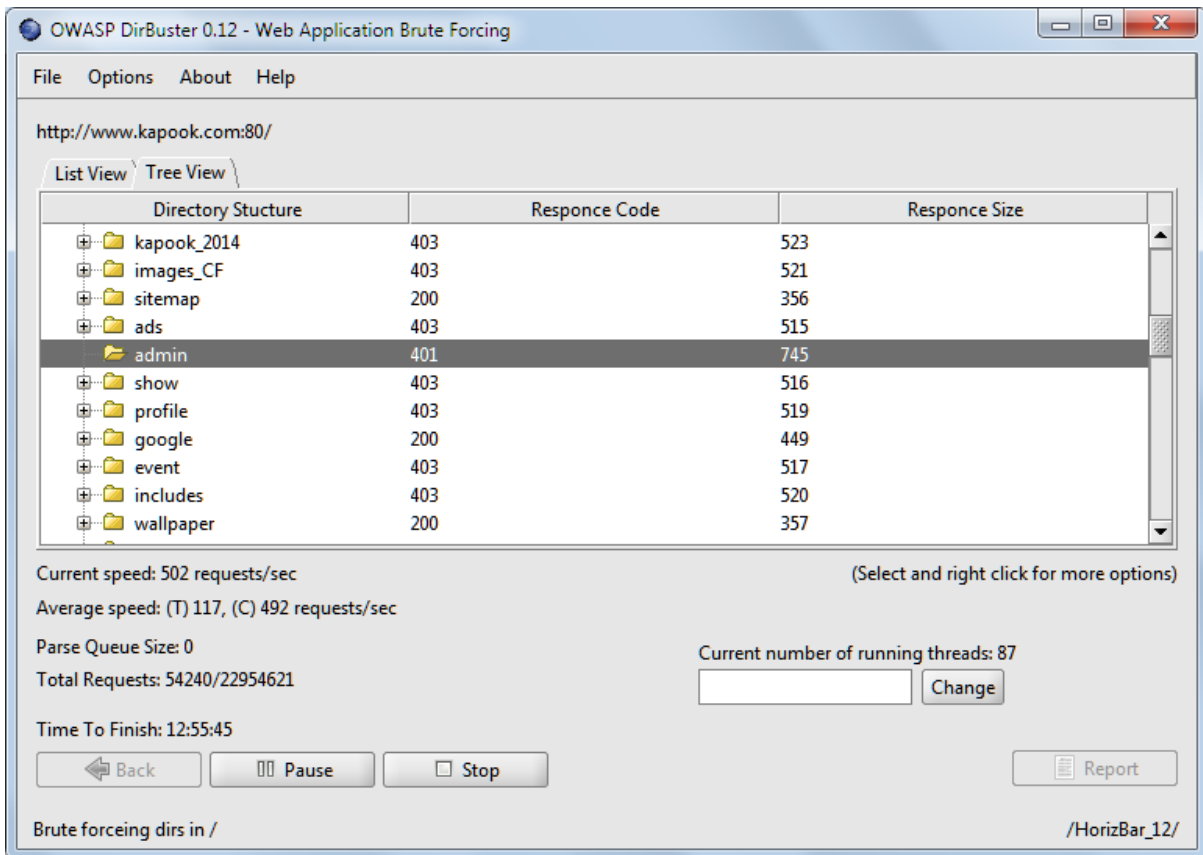
7. จะปรากฏไฟล์โดเมนหรือทั้งหมดที่มีอยู่ใน <http://www.kapook.com>



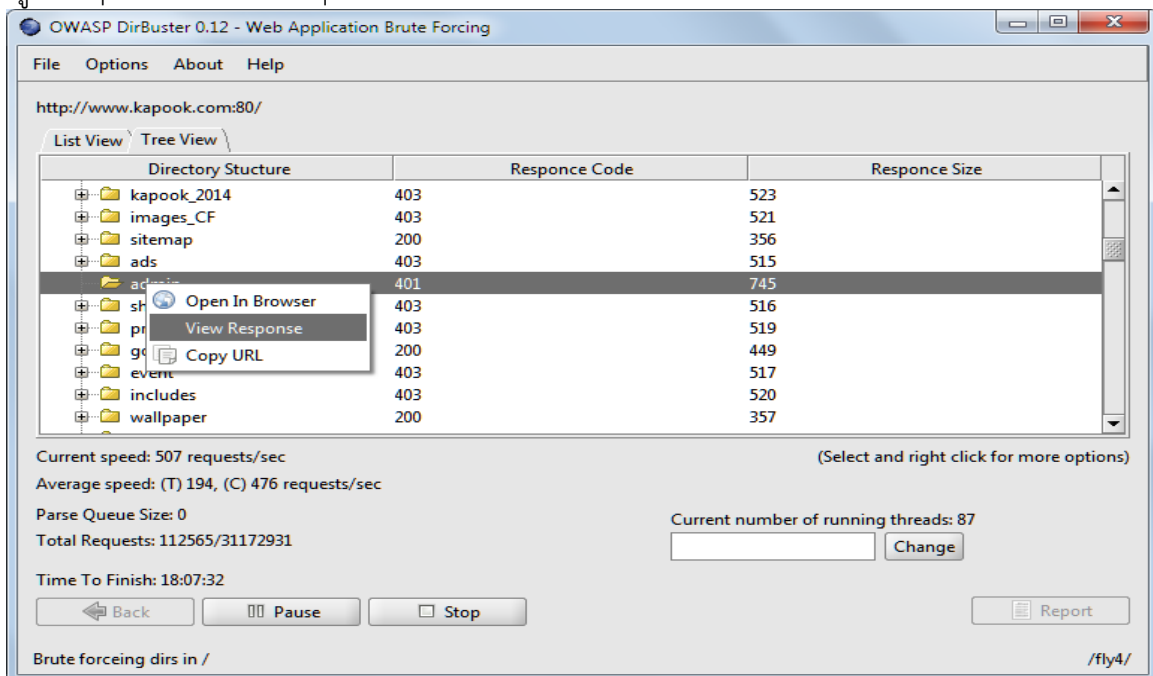
8. ถ้าคลิกเลือกที่ Tree View จะแสดงเป็นไฟล์ folder ต่างๆ



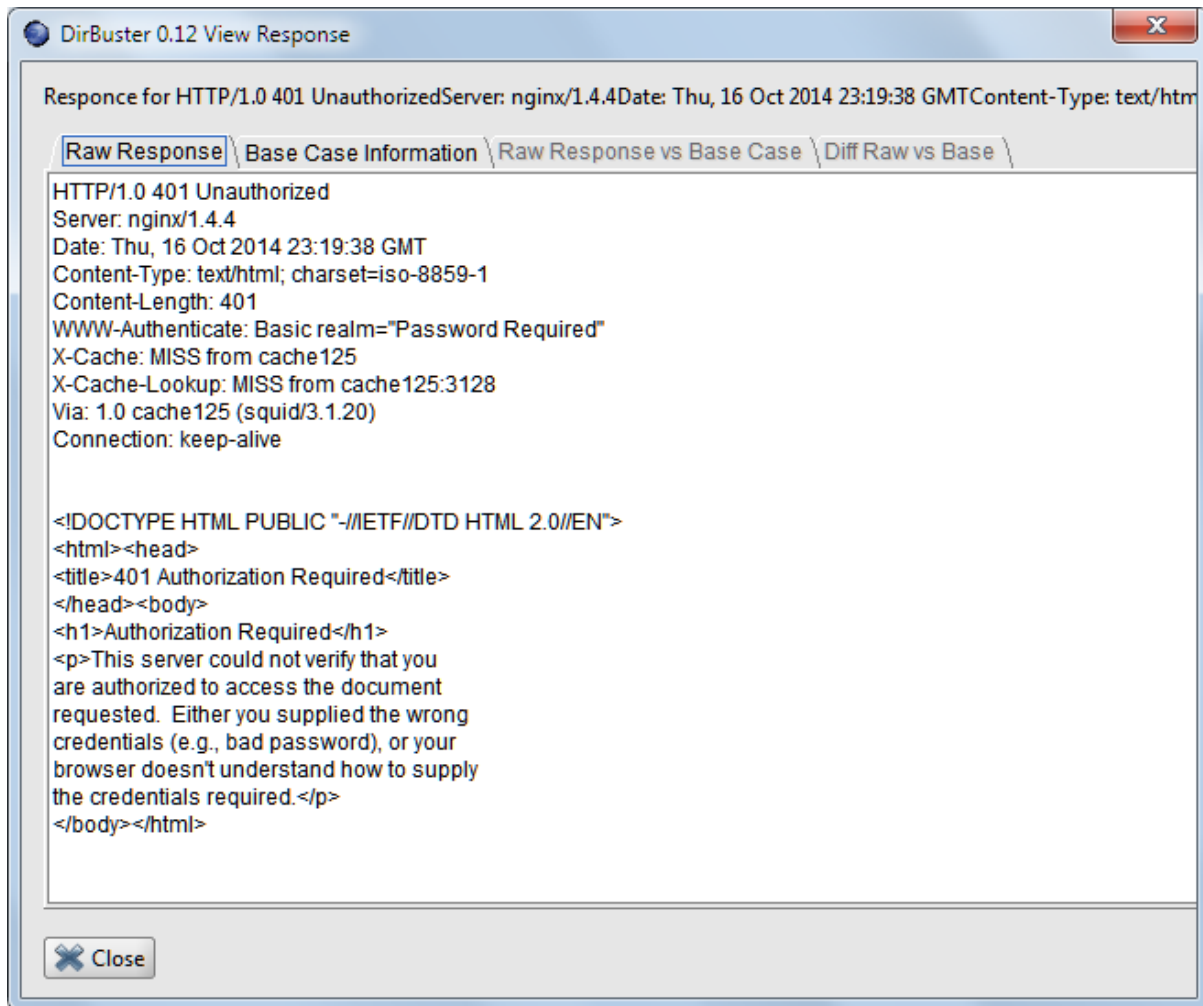
9. สามารถเลือกไฟล์ที่เราต้องการดูข้อมูลได้



10. ถ้าต้องการดูข้อมูลของไฟล์นั้นๆ ให้ทำการคลิกขวาที่ไฟล์แล้วเลือก View Response ก็จะแสดงข้อมูลต่างๆ ของไดเรกทอรีนั้นๆ

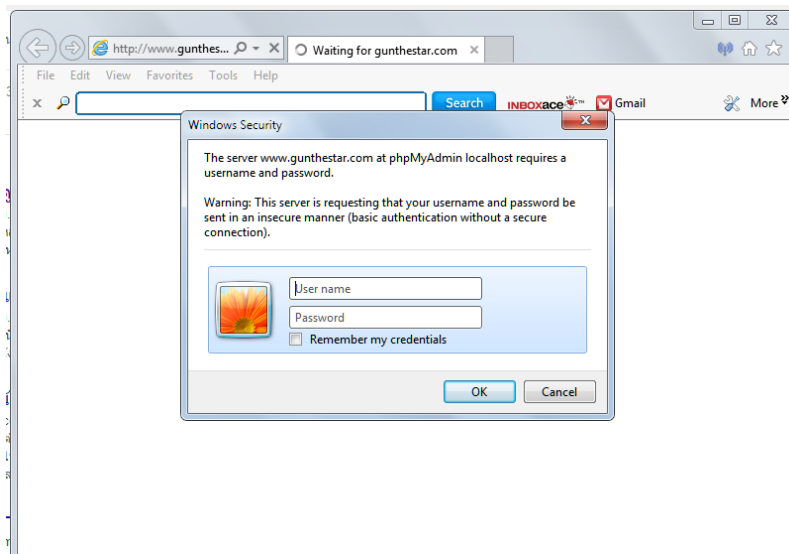


11. เมื่อคลิกเลือก View Response แล้วจะปรากฏข้อมูลดังรูป

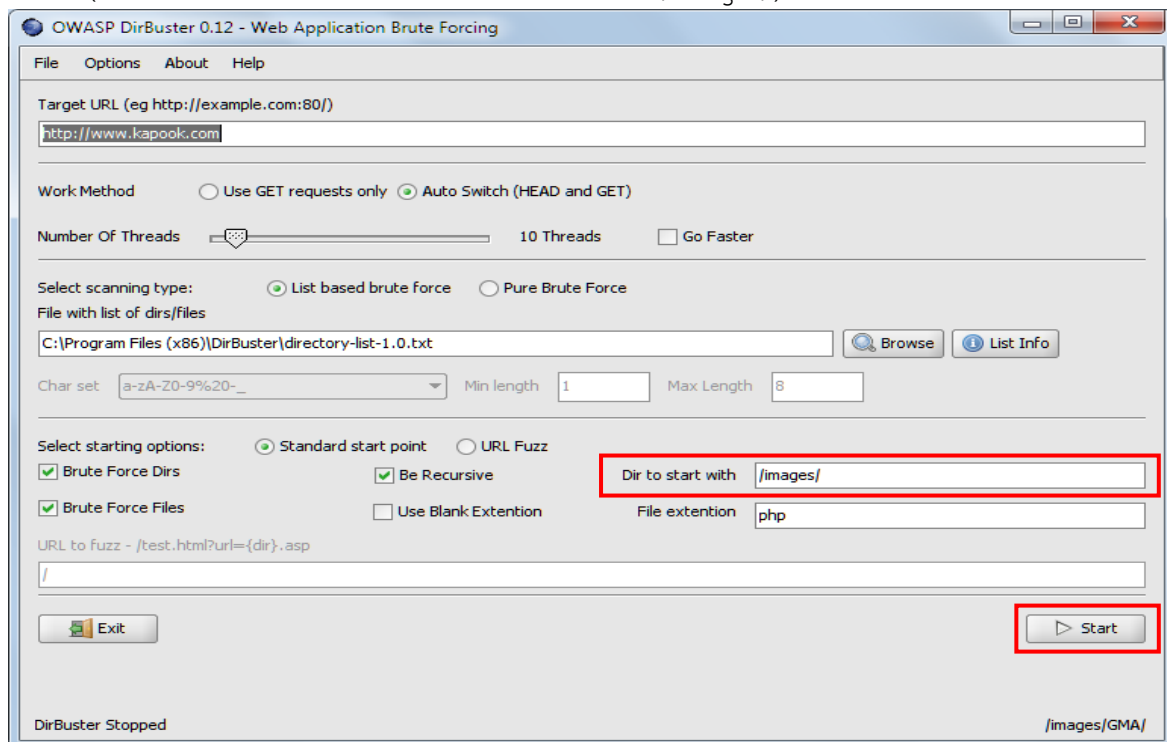


Note : กรณีที่ค้นหาแล้วพบไดเรกทอรี /phpmyadmin/ ถ้าทราบ username และ password ก็จะสามารถเข้าไปดูข้อมูลในฐานข้อมูลนั้นได้ แต่ถ้าไม่ทราบก็ไม่สามารถเข้าไปดูข้อมูลในฐานข้อมูลนั้นได้เช่นกัน และในกรณี

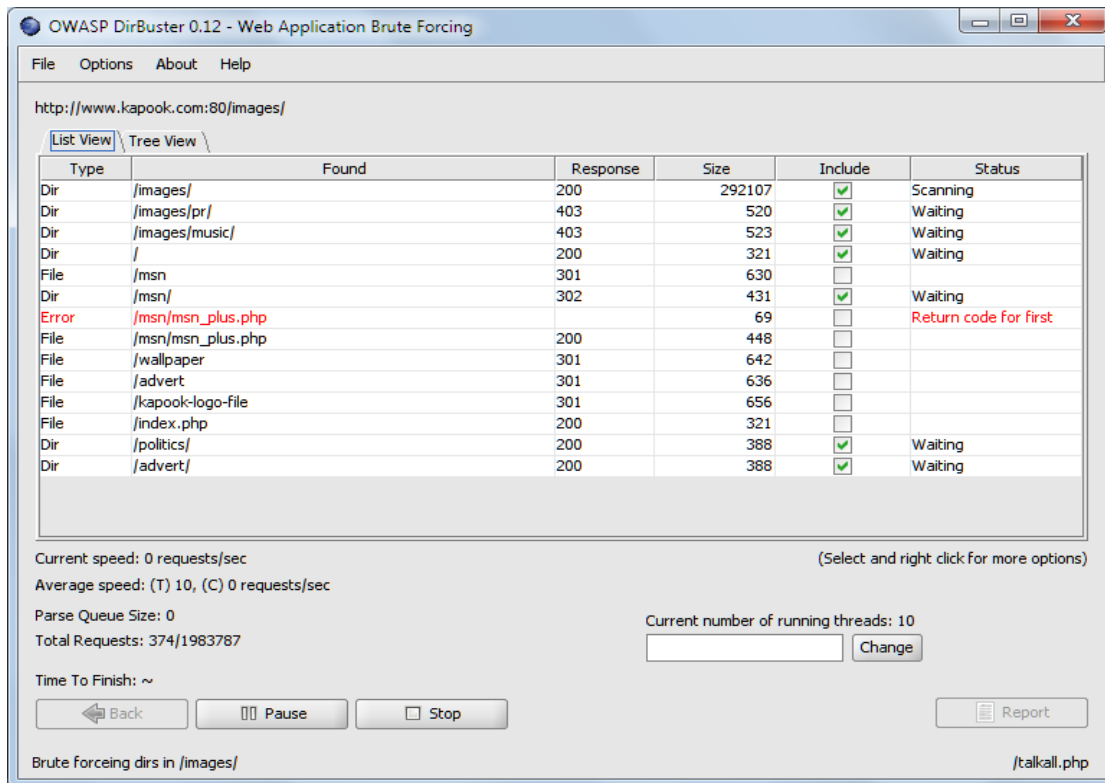
ที่ค้นหาแล้วพบไดเรกทอรี /phpmyadmin/ ถ้าฐานข้อมูลนั้นไม่ได้ตั้งค่า username และ password ไว้ก็สามารถเข้าไปดูข้อมูลในฐานข้อมูลนั้นได้เลย



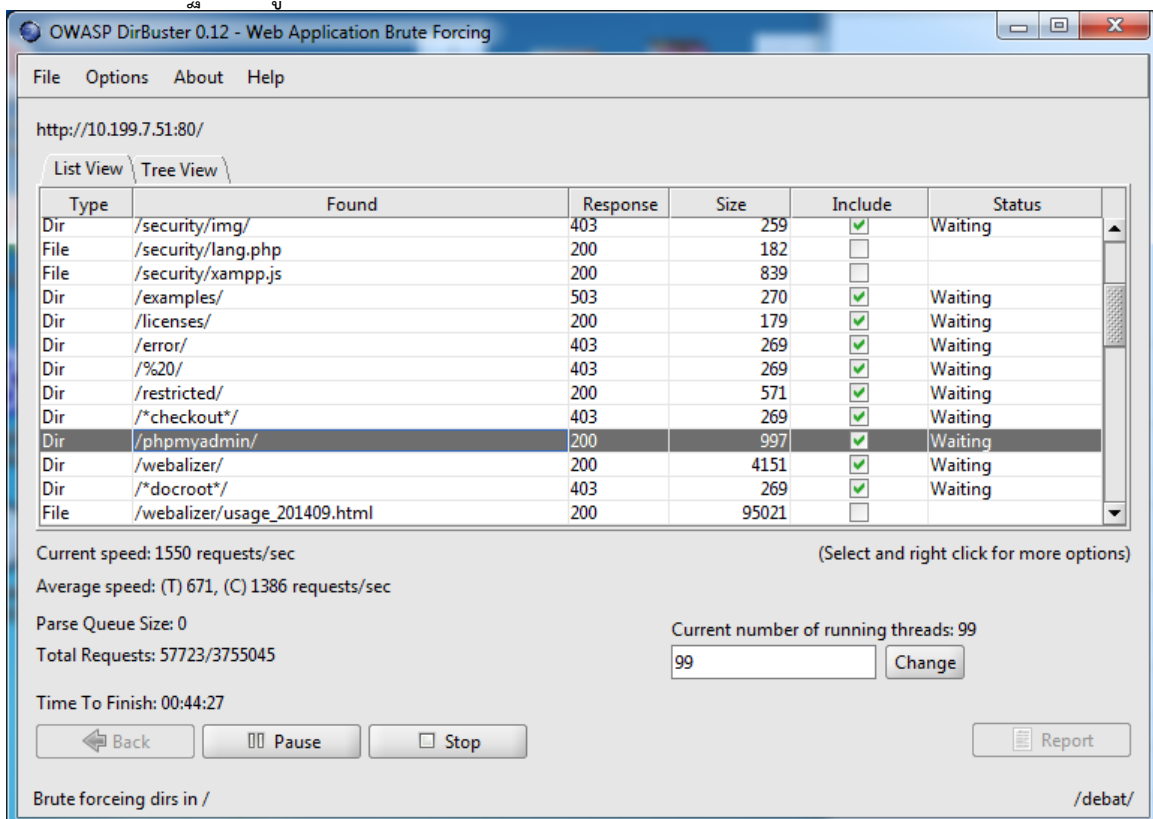
12. ในส่วนของ Dir to start with เป็นการค้นหาไดเรกทอรีเฉพาะที่เราต้องการค้นหา โดยนำชื่อไดเรกทอรีที่เราต้องการค้นหากรอกใส่ในช่องนี้ได้เลย จากนั้นกดปุ่ม Start เพื่อค้นหาไดเรกทอรีที่เราต้องการ (ตัวอย่างเช่น ต้องการที่จะค้นหาไดเรกทอรีที่มีชื่อว่า /images/)



13. โปรแกรมจะทำการค้นหาไฟล์ที่เกี่ยวข้องกับไดเรกทอรีที่มีชื่อว่า /images/ ดังรูป



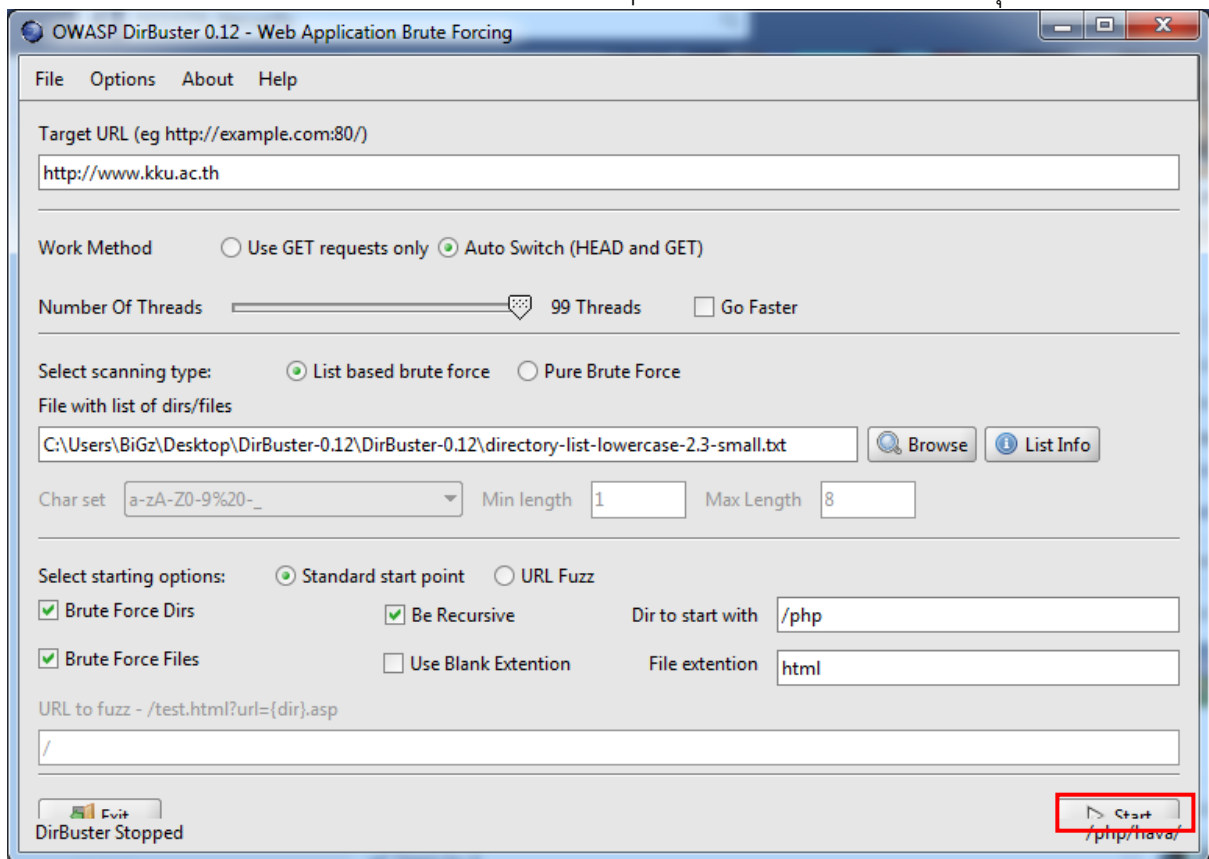
14. ตัวอย่างการค้นหาไฟล์ในไดเรกทอรีของ <http://10.199.7.51:80/> และเลือก /phpmyadmin/ ในไดเรกทอรีที่เป็นฐานข้อมูล



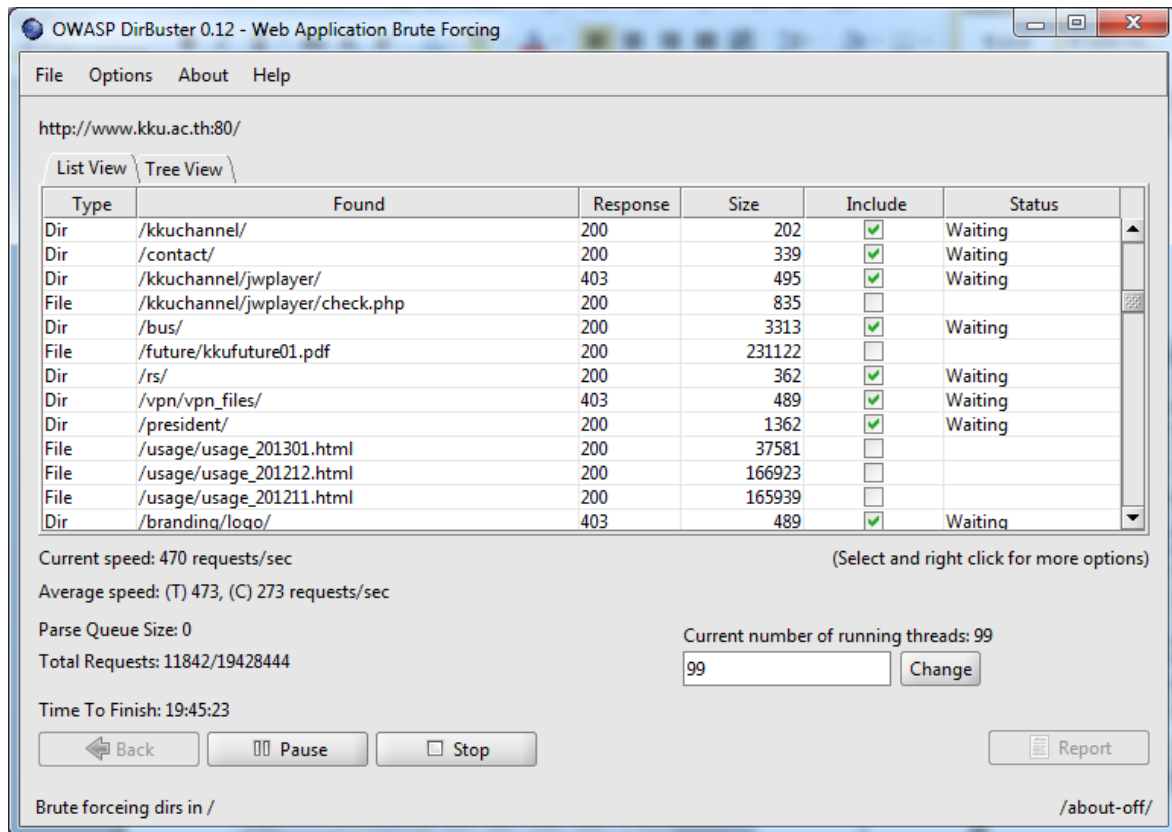
15. จากนั้นจะปรากฏหน้าของฐานข้อมูลที่ได้จากการเลือกไดเรกทอรี /phpmyadmin/

LId	User	Pwd	FName	LName	Sex	Tel	Email
1	psk	1234	SMJ	PSK	M	258258	smj#kkhhf
2	ixuou	123456	Songvut	Butham	M	0843928845	ixuou@ixuou.com
3	htz	k010437	kan	kanchanok	f	080 080 08	tanniiz.i.vip@gmail.com
4	kritanon	123456	kritanon	Sangchompo	m	0883342133	Bm_hi-school@hotmail.com
5	xeer	xeer	krisana	pimpanit	m	0966742680	killazaold1993@gmail.com
6	Constantum	816214	kittinut	private	m	0831298728	kittinut_p@kumail.com
7	kanok	123456789	kanokpom	martkaew	f	0800000000	kanok@gmail.com
8	poohpan	4568363	Apichit	Tischob	m	0876768282	poohpanbakery@live.com
9	jane	242536	Chenchira	Thabphuta	F	0832868024	janejane24@hotmail.co.th
10	Gubenza	123456789	Piyawat	Namwanta	M	0833333333	Gubenza@hotmail.co.uk
11	Jeab	0833568037	Tatiya	Ouakan	F	0922658037	T_A_T_L_Y_A@hotmail.com
12	axeger001	12345	phuwanai	puangmalai	M	1234567890	axeger001@hotmail.com
13	wasitaaa	1409901044990	wasita	yotachai	f	0823017415	wasitaaa_9999@hotmail.com
14	kanokpo	123456	kanok	zxcvbn	f	0800000000	ka@gmail.com
15	Pongpang	2112	Napaporn	Jinsaeng	F	0831415691	pang_9989@hotmail.com
16	Waraporn	02112536	Waraporn	Neatprom	F	0801956808	ariwiw@hotmail.com
17	ing	291036	ketsuda	pholnamin	f	0812558377	ketsudaing@gmail.com
18	numm	num999999999	kliapan	ledsanchai	f	0000000000	manju47341@gmail.com
19	akrapol	1234	akrapol	akrapol	m	1234	ak@gmail.com
20	maewmie	123456789	maewmie	memy	F	0821234567	memy090909@gmail.com
21	TAPLONY	12345	RATCHANON	CAHOPOOBUT	1	111111	mail
22	lipungpingil	123456	Nadhapa	Tonongpan	F	0804115733	spk_kps_01@hotmail.com
23	touiz	1234	Narong	Bodee	M	0834449999	staciz@hotmail.com
24	Mavmatposri	imav668	Waraporn	Matposri	F	088-999999	mav_matposri@hotmail.com

16. ตัวอย่างการค้นหาไฟล์ไต่แรกทอรีของ <http://www.kku.ac.th> จากนั้นกดปุ่ม Start



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



18. เมื่อกดเลือกที่ไฟล์ /usage/usage_201301.html แล้ว จะปรากฏข้อมูลดังรูป

Monthly Statistics for January 2013		
Total Hits		6857
Total Files		4564
Total Pages		6386
Total Visits		9
Total KBytes		2275
Total Unaqe Sites		2
Total Unaqe URLs		1
Total Unaqe Referrers		1
Total Unaqe 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		
Code 200 - OK	66.58%	4564
Code 403 - Forbidden	33.44%	2293

สรุป

ในบทเรียนนี้ได้อธิบายถึงวิธีการติดตั้งและการใช้งานของโปรแกรม DirBuster ซึ่งเป็นโปรแกรมที่ใช้ค้นหาไดเรกทอรีต่างๆ 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>

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