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 มีลักษณะการทำงานคือจะเข้าไปค้นหาไดเรกทอรีต่างๆ ที่ซ่อนอยู่ใน web sever โดยที่หน้า web sever ยังมีการใช้งานได้เป็นปกติ

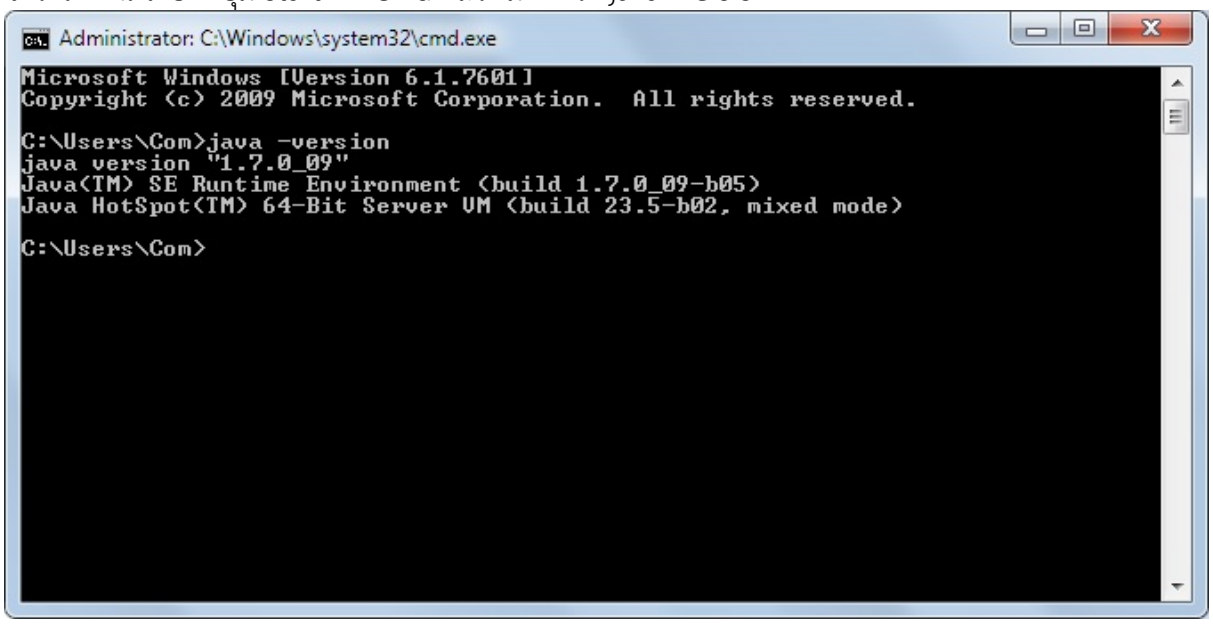
คุณสมบัติ

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

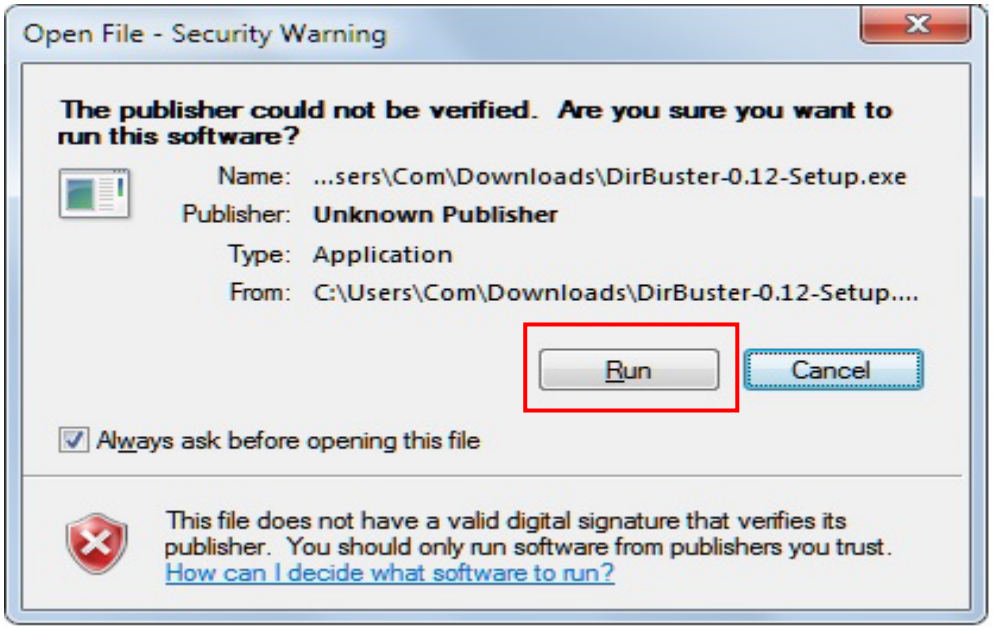
- **การติดตั้งโปรแกรม DirBuster**

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

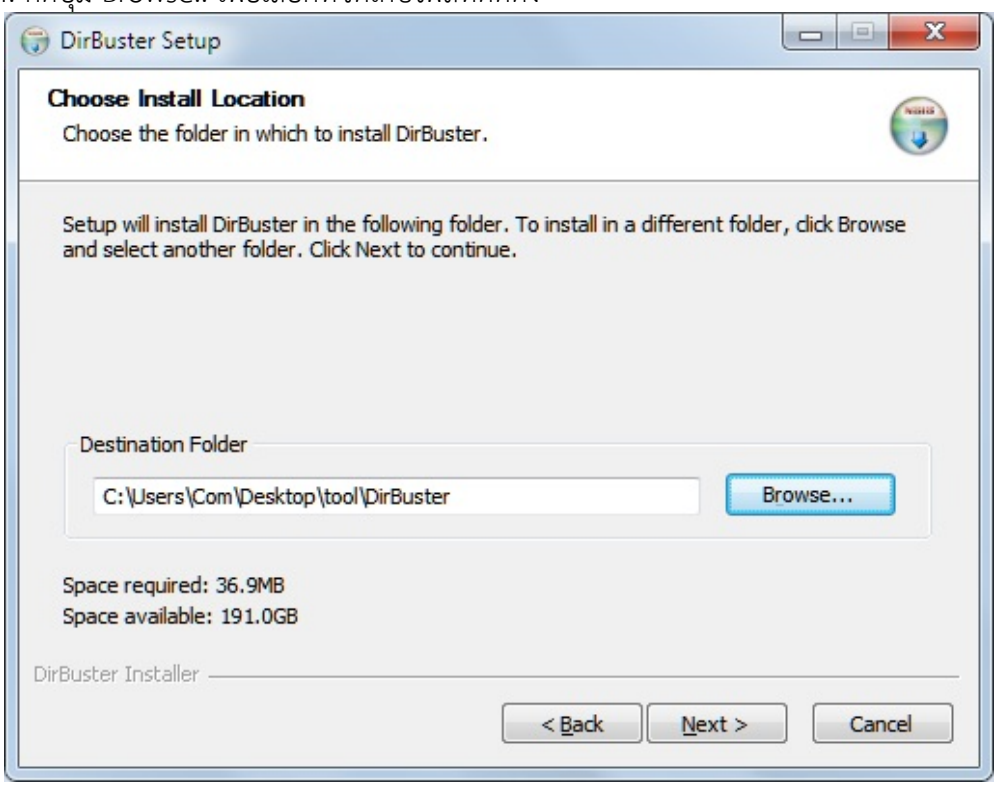
2. ก่อนที่จะทำการติดตั้งโปรแกรม DirBuster-0.12-Setup.exe นั้น ผู้ใช้ต้องทำการตรวจสอบเครื่องผู้ใช้ก่อนว่ามีโปรแกรมจาวาหรือไม่ ถ้าไม่มีให้ทำการติดตั้งโปรแกรมจาวาก่อน สามารถตรวจสอบดูโปรแกรมจาวาได้ดังนี้ โดยกดปุ่ม start >> cmd แล้วพิมพ์คำว่า java -version



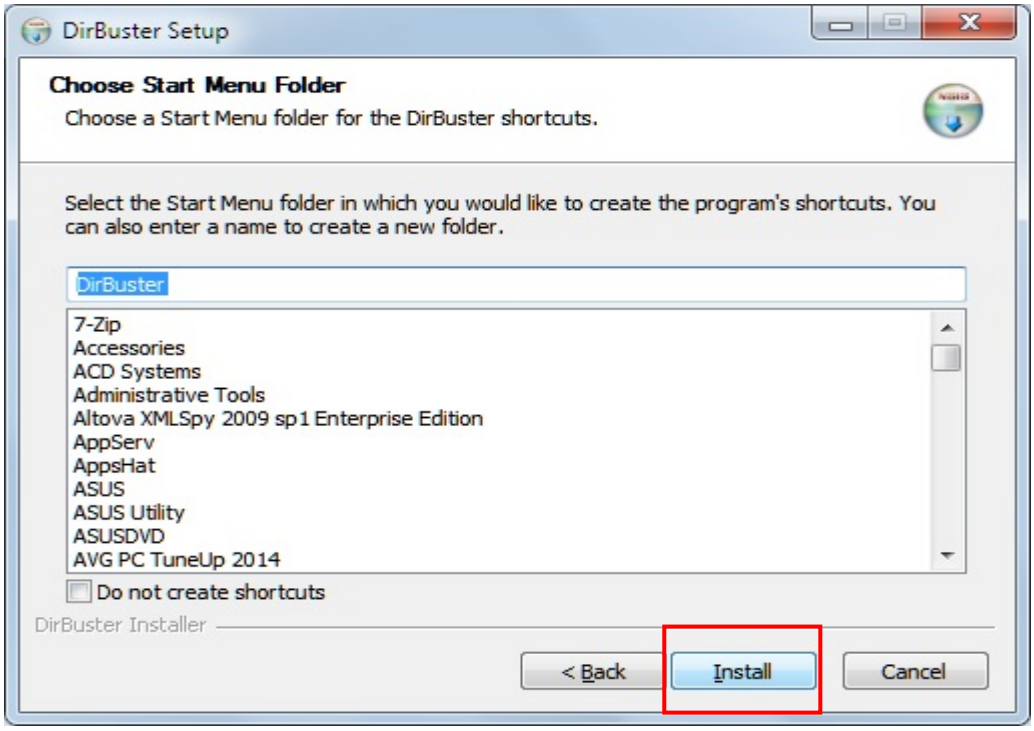
3. เมื่อ download เรียบร้อยแล้ว ให้ทำการติดตั้งโปรแกรม DirBuster-0.12-Setup.exe โดยกดปุ่ม Run



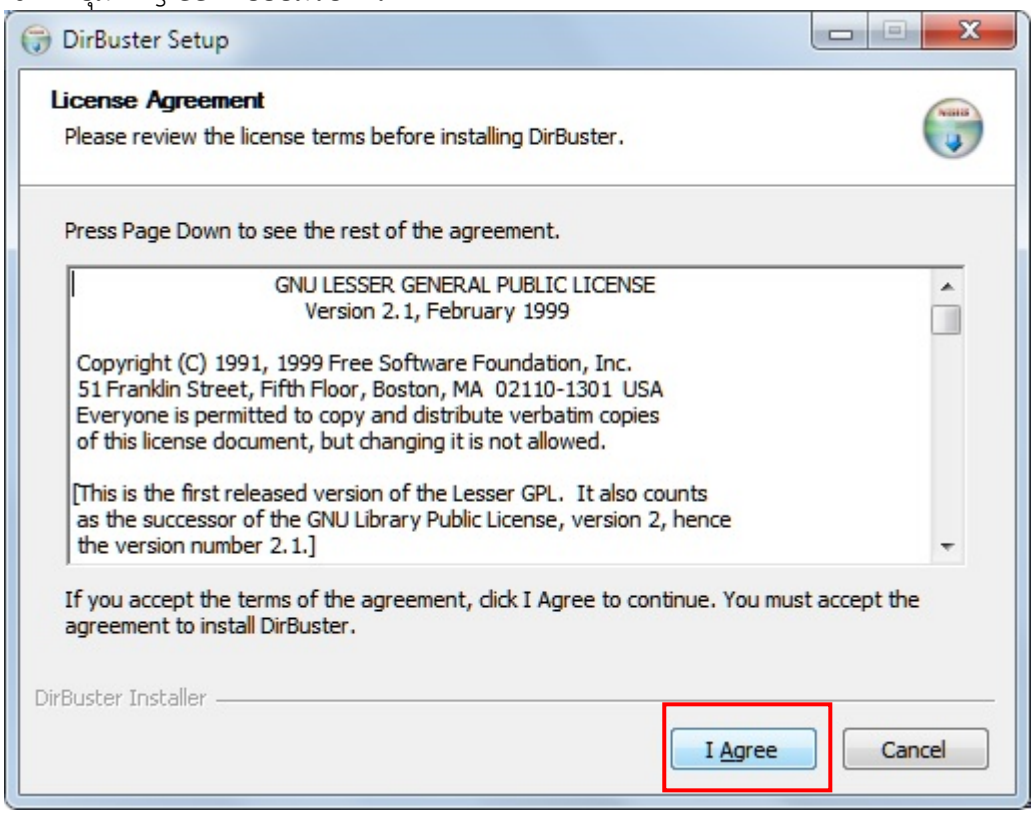
4. กดปุ่ม Browse.. เพื่อเลือกที่จัดเก็บไฟล์ที่ติดตั้ง



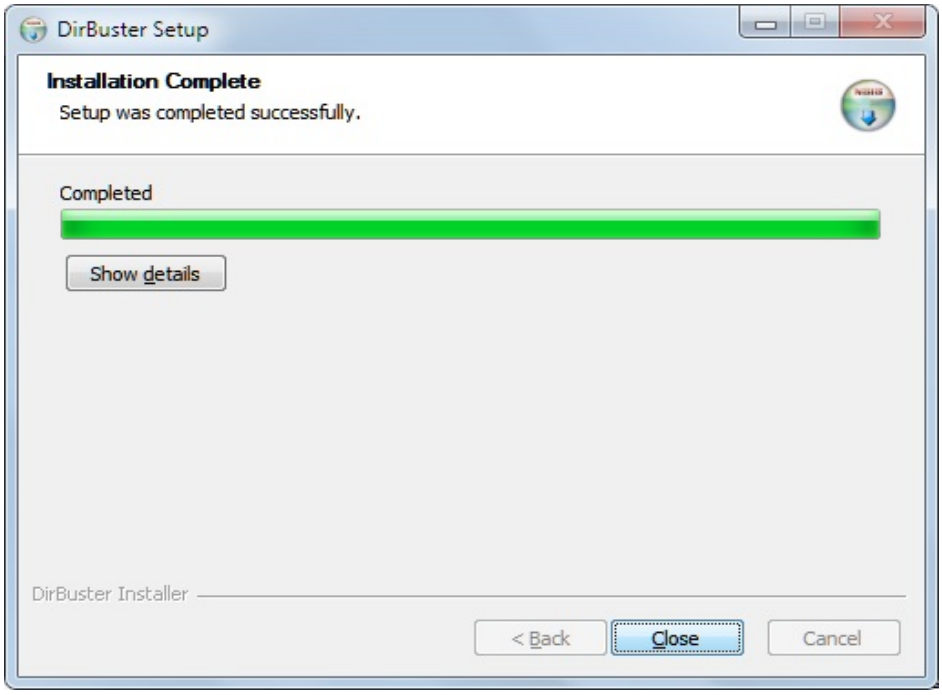
5. เมื่อเลือกที่จัดเก็บไฟล์เรียบร้อยแล้ว ให้กดปุ่ม Install เพื่อติดตั้ง



6. กดปุ่ม I Agree เพื่อยอมรับการติดตั้ง

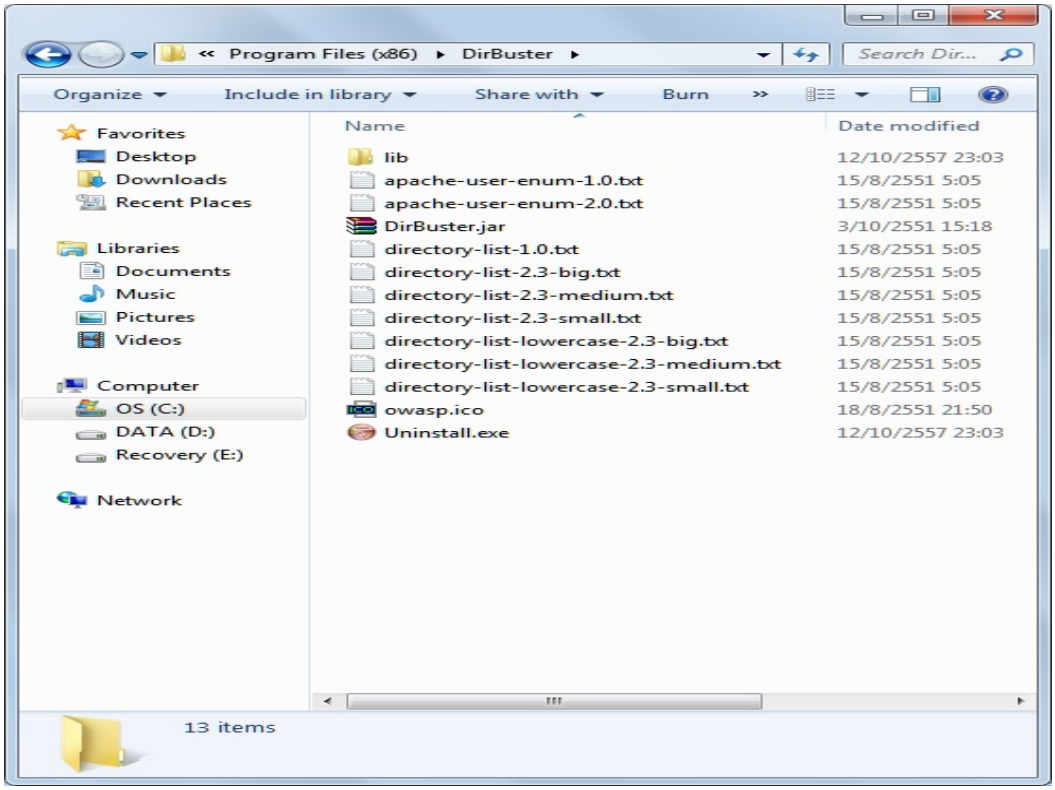


7. ดำเนินการตามขั้นตอนจนปรากฏหน้าจอ Installation Complete ซึ่งแสดงถึงการการติดตั้งโปแกรมเสร็จสมบูรณ์

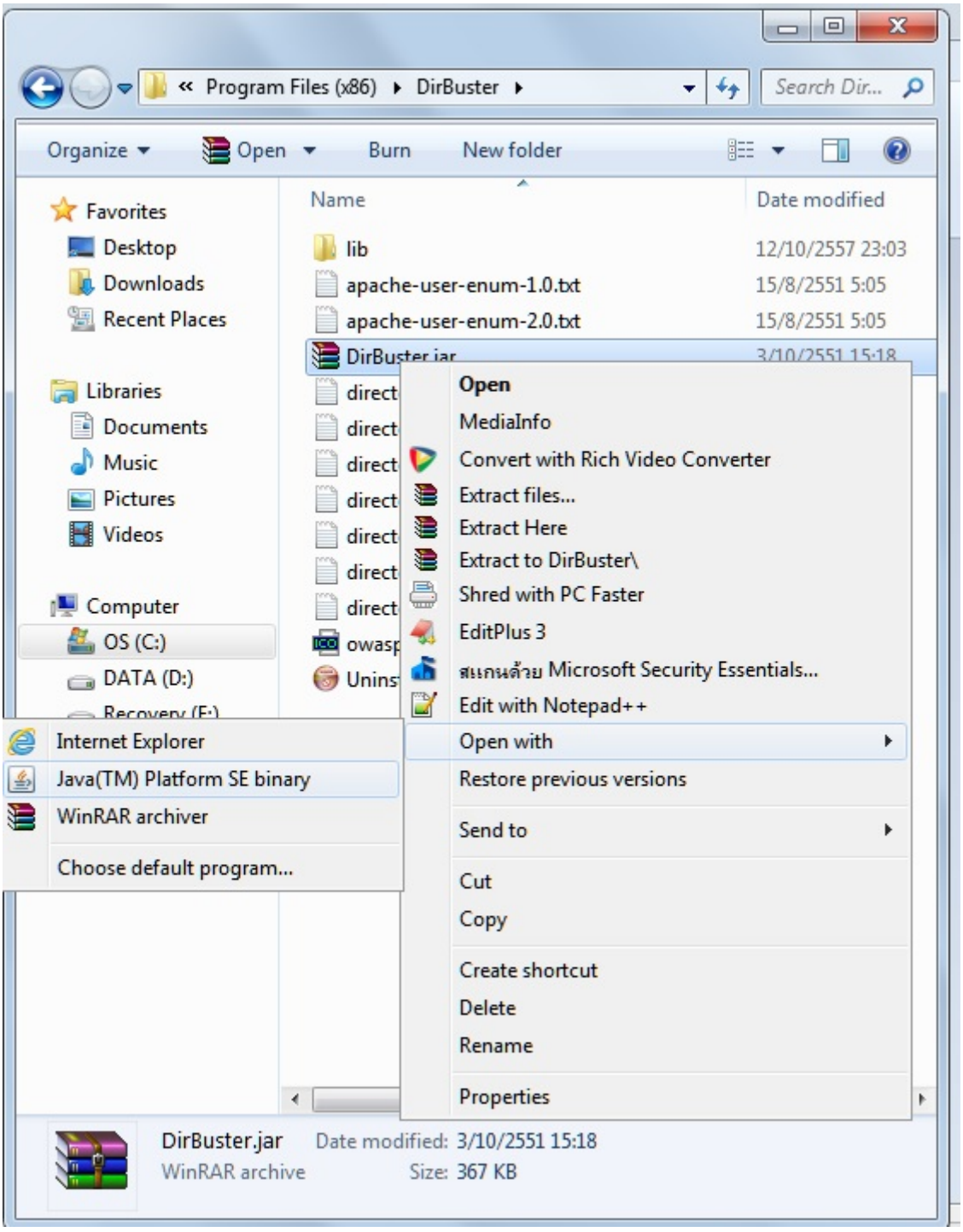


- **การใช้งานโปรแกรม DirBuster**

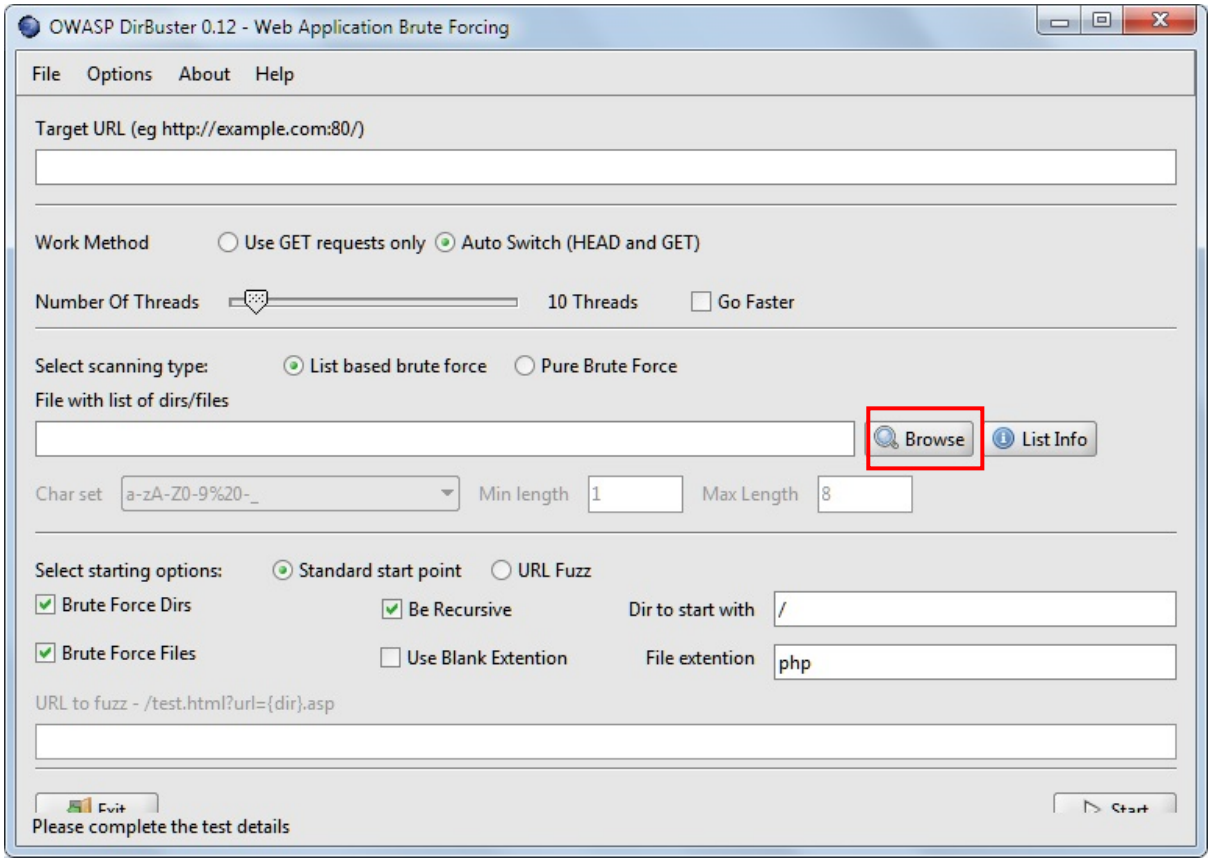
1. เปิดโปรแกรม DirBuster ที่ติดตั้งสำเร็จ



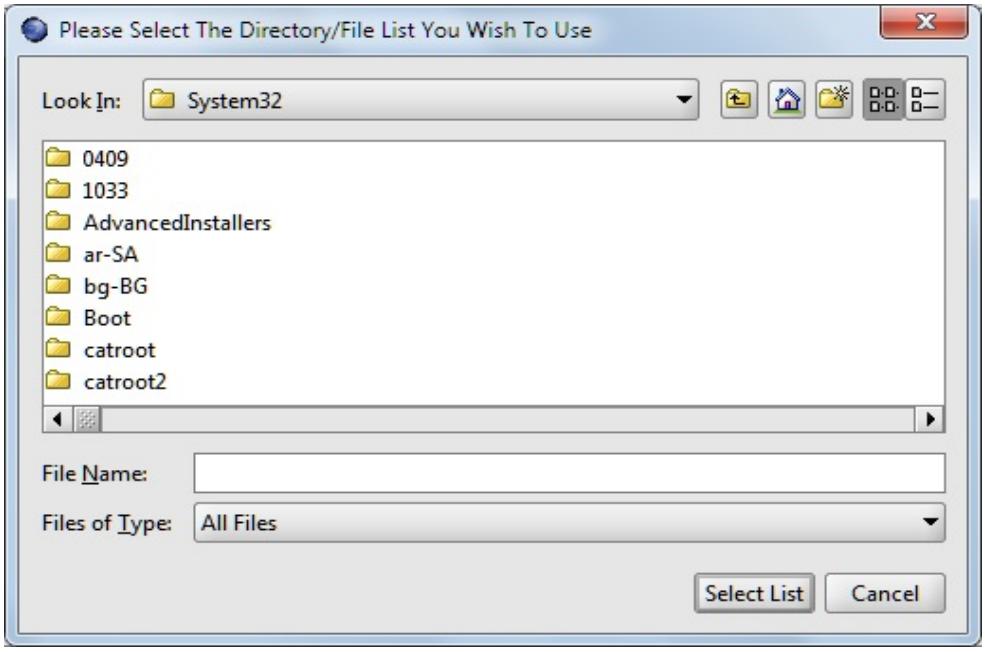
2. เมื่อเปิดโปรแกรมแล้ว ให้คลิกขวาที่ DirBuster.jar แล้วเลือก Open with >> Java(TM) Platform SE binary



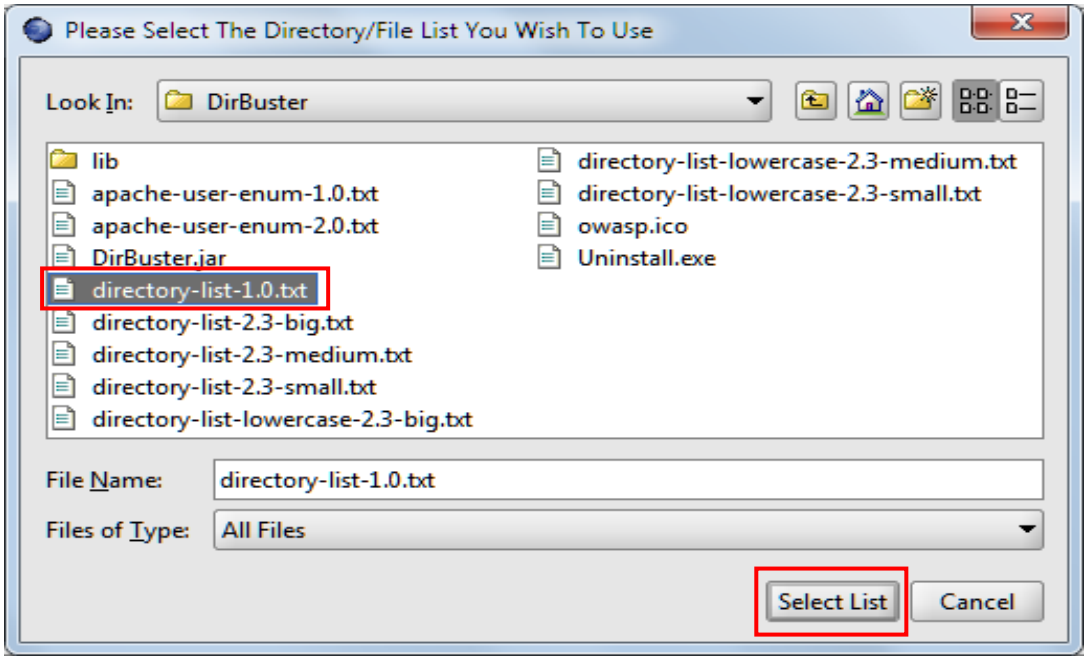
3. จะปรากฏหน้าโปรแกรม DirBuster ขึ้นมาดังรูป จากนั้นให้กดปุ่ม Browse เพื่อเลือกไฟล์ที่จัดเก็บโปรแกรม DirBuster ไว้



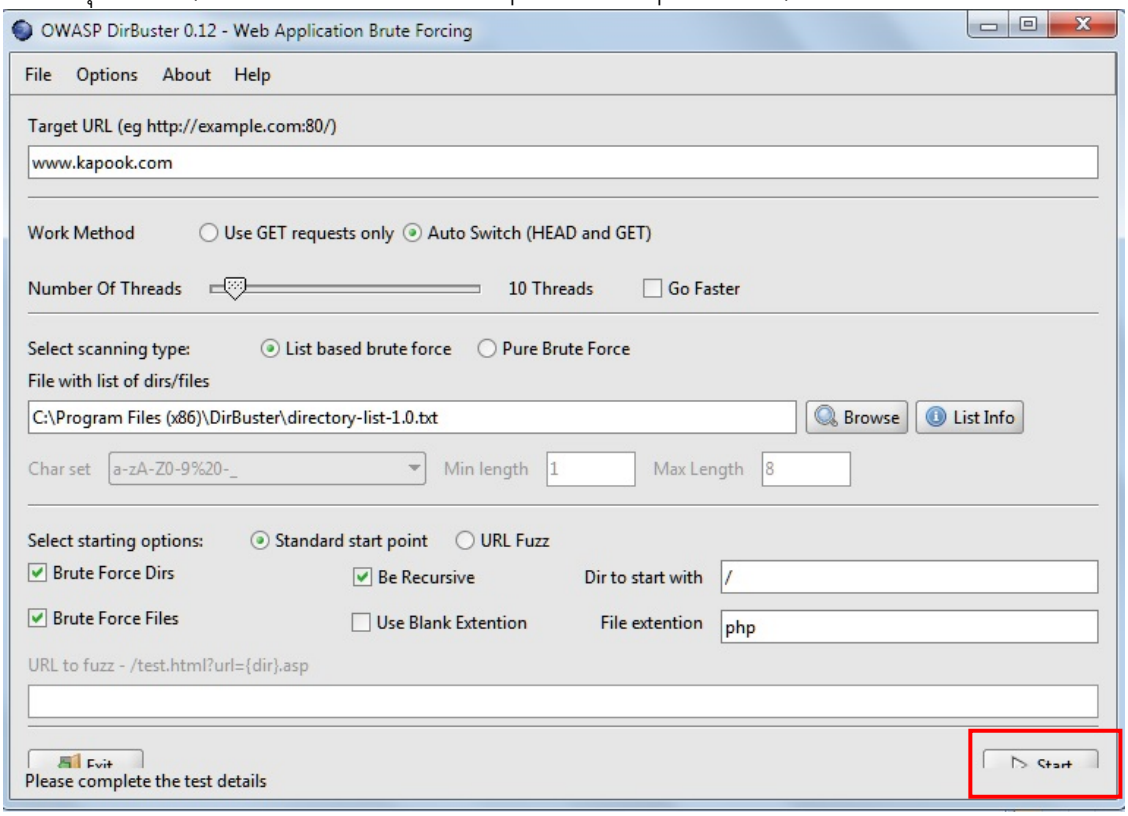
4. ให้เลือกไฟล์ที่จัดเก็บโปรแกรม DirBuster ไว้



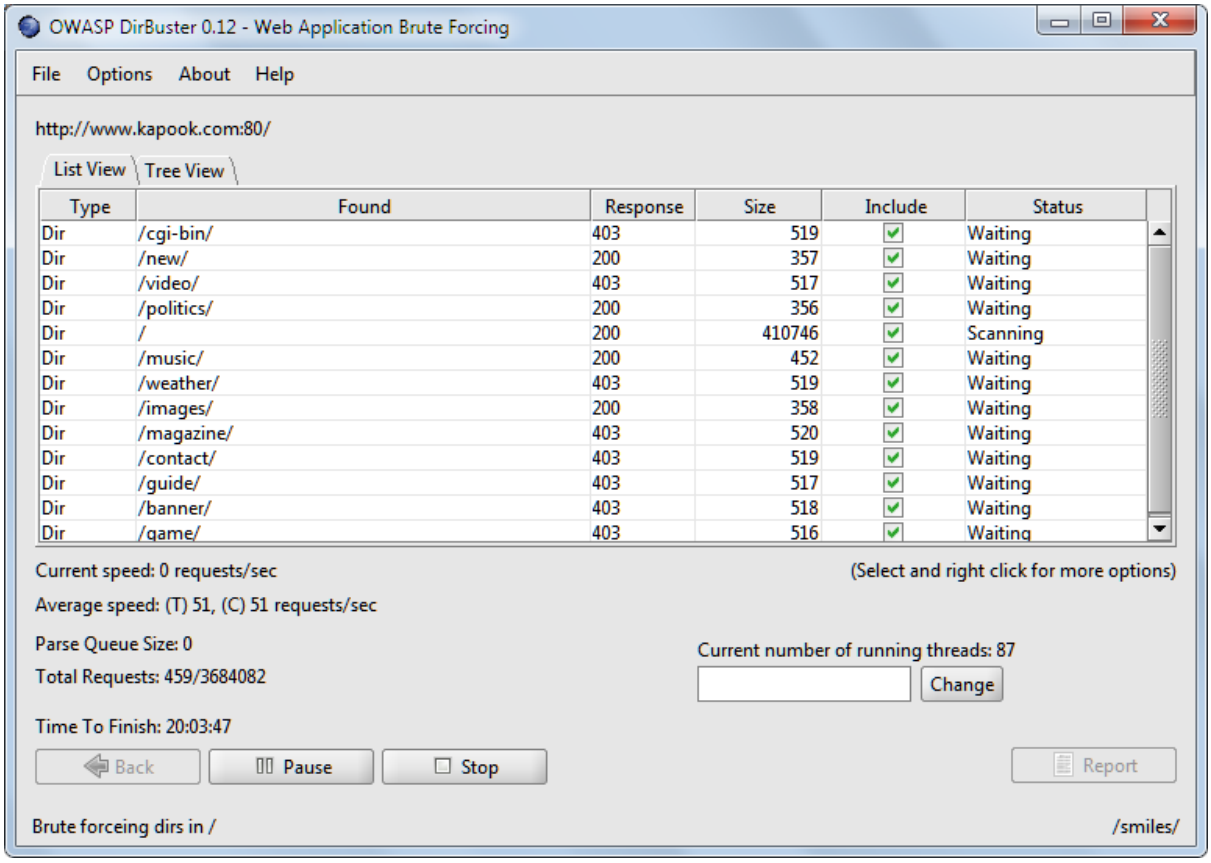
5. ให้คลิกเลือก directory-list-1.0.txt เพื่อแสดงข้อมูลไฟล์ออกมาที่ไดเรกทอรี แล้วกดปุ่ม Select List



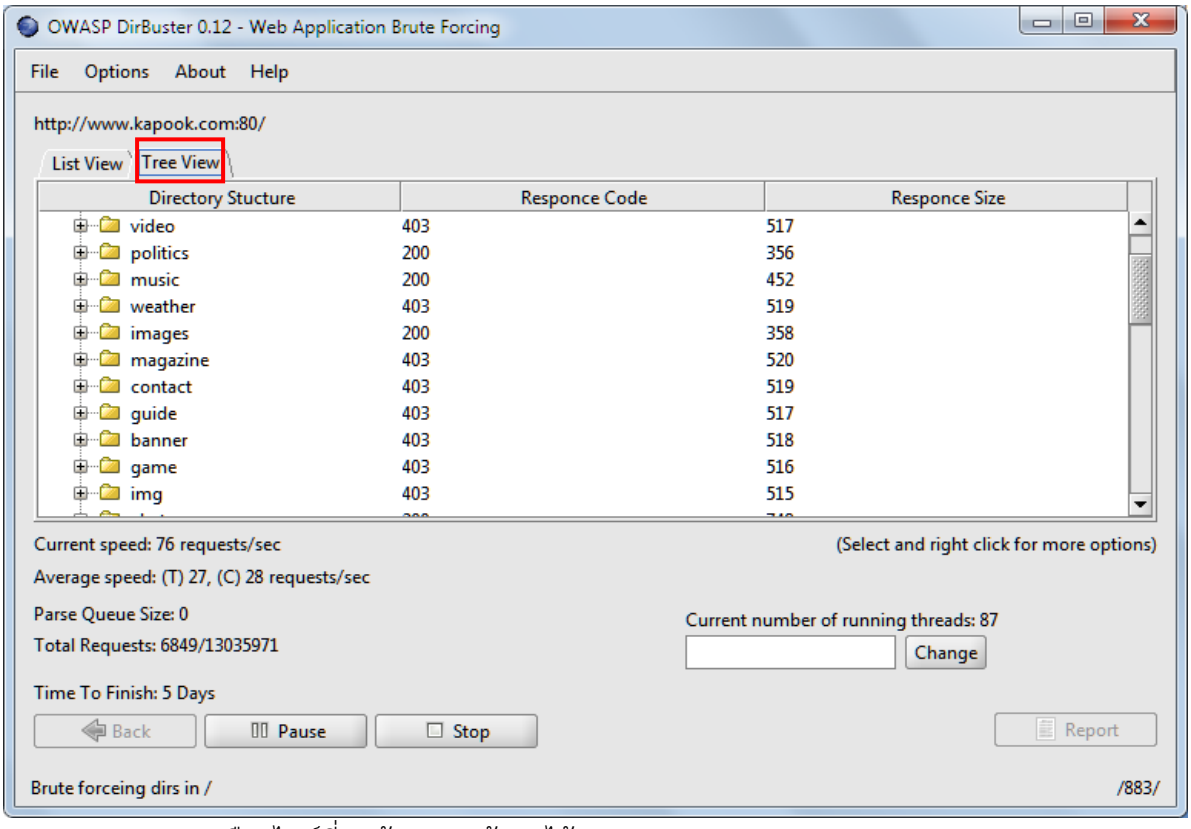
6. จากนั้นจะปรากฏหน้าดังรูป ให้ทำการกรอก URL ที่เราต้องการเข้าไปดูข้อมูลไฟล์ในไดเรกทอรี จากนั้นกดปุ่ม Start (ในตัวอย่างนี้เป็นเว็บไซต์ http://www.kapook.com)



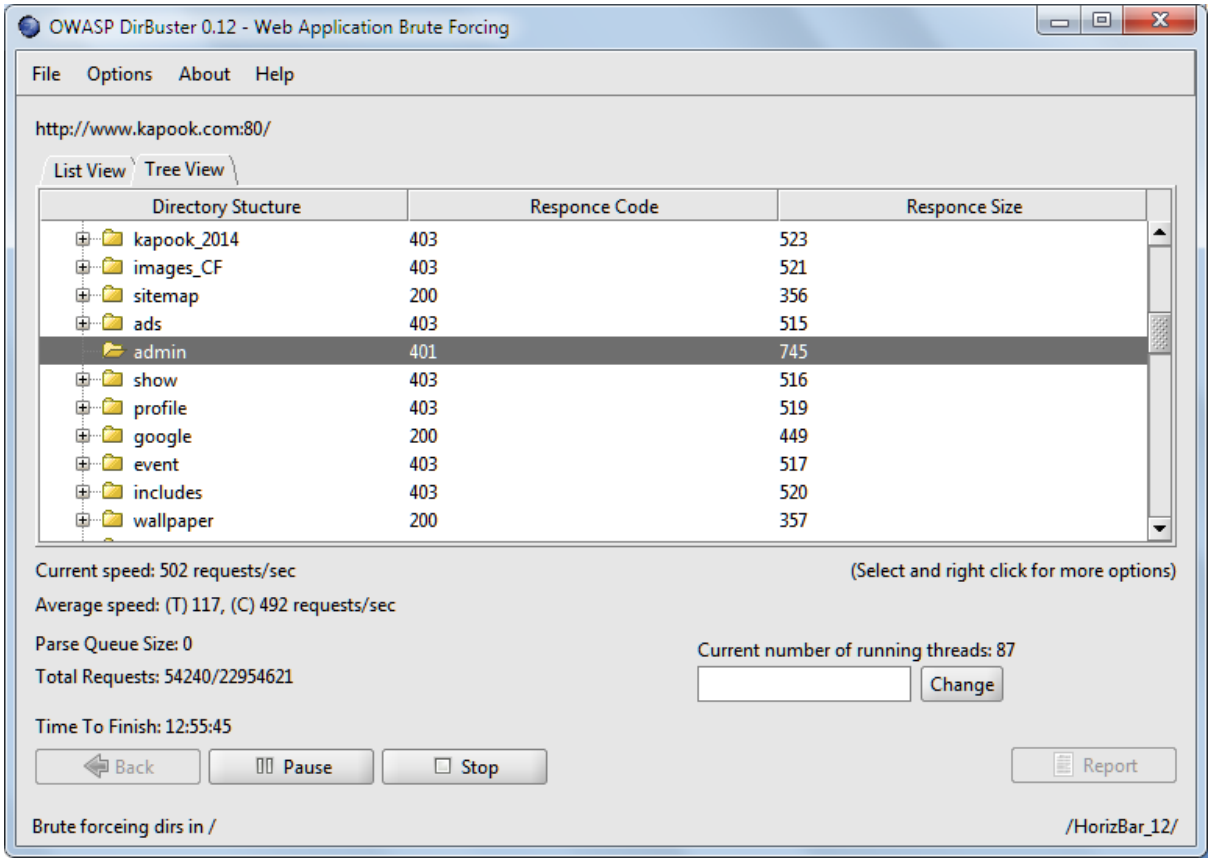
7. จะปรากฏไฟล์ไดเรกทอรีทั้งหมดที่มีอยู่ใน http://www.kapook.com



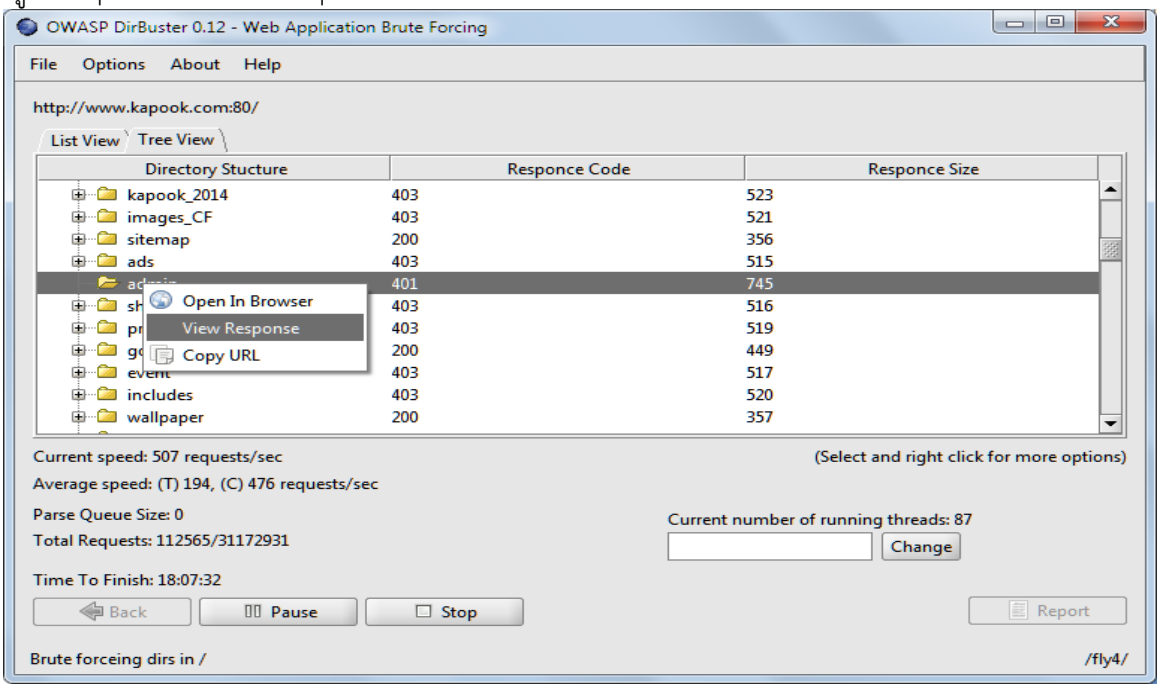
8. ถ้าคลิกเลือกที่ Tree View จะแสดงเป็นไฟล์ folder ต่างๆ



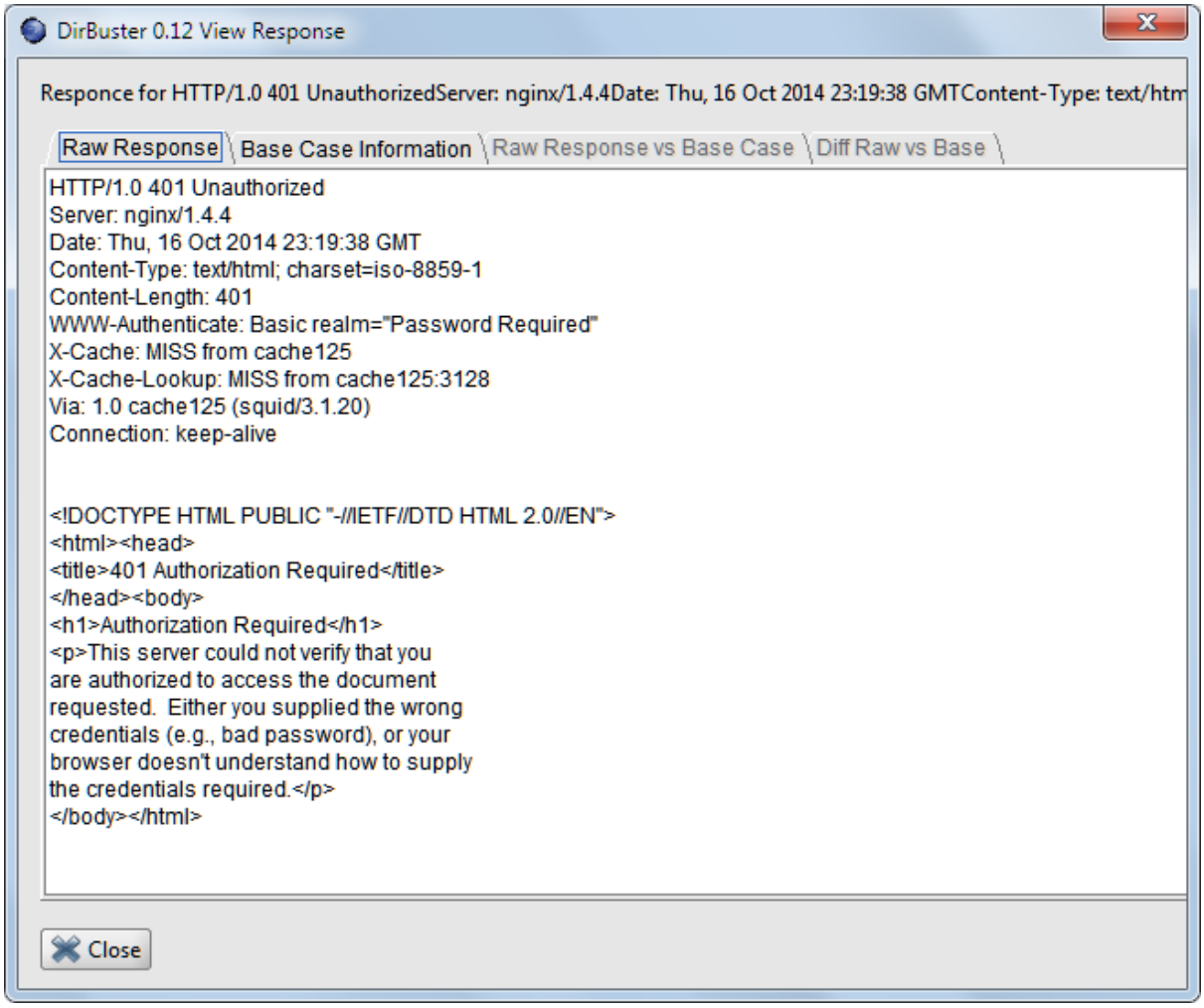
9. สามารถเลือกไฟล์ที่เราต้องการดูข้อมูลได้



10. ถ้าต้องการดูข้อมูลของไฟล์นั้นๆ ให้ทำการคลิกขวาที่ไฟล์แล้วเลือก View Response ก็จะแสดงข้อมูลต่างๆ ของไดเรกทอรีนั้นๆ

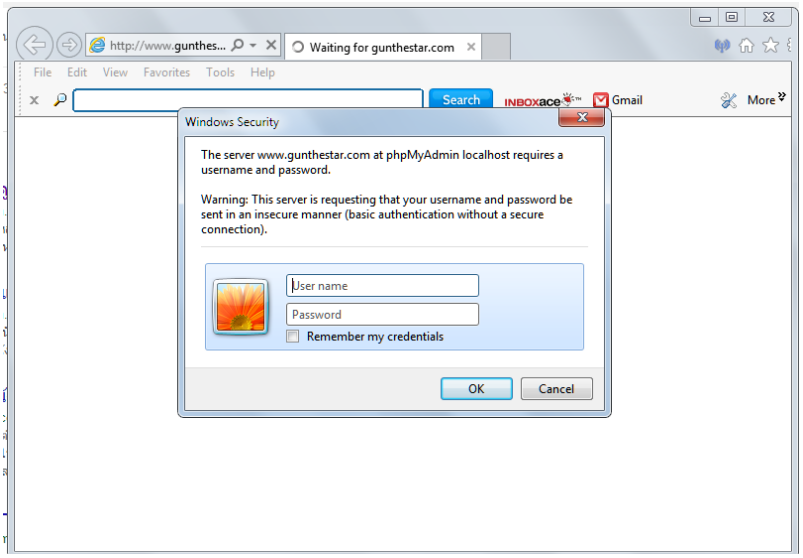


11. เมื่อกดเลือก View Response แล้วจะปรากฏข้อมูลดังรูป

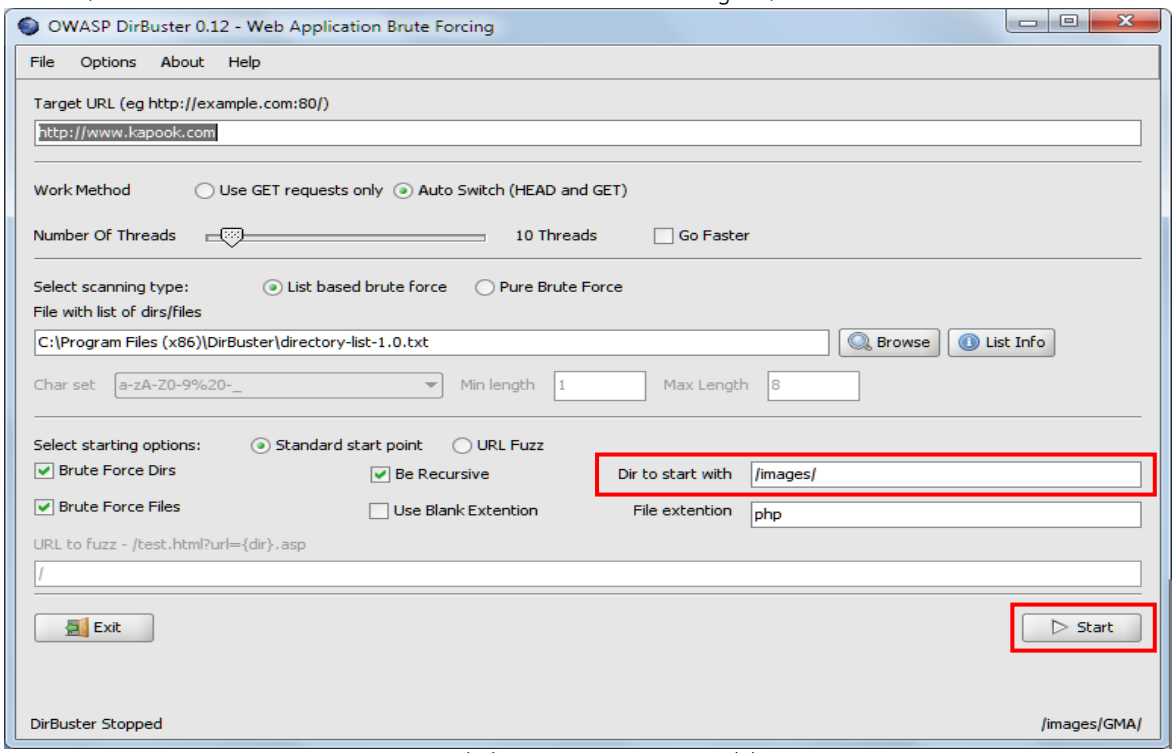


Note : กรณีที่ค้นหาแล้วพบไดเรกทอรี่ /phpmyadmin/ ถ้าทราบ username และ password ก็สามารถเข้าไปดูข้อมูลในฐานข้อมูลนั้นได้ แต่ถ้าไม่ทราบก็ไม่สามารถเข้าดูข้อมูลในฐานข้อมูลนั้นได้เช่นกัน และในกรณี

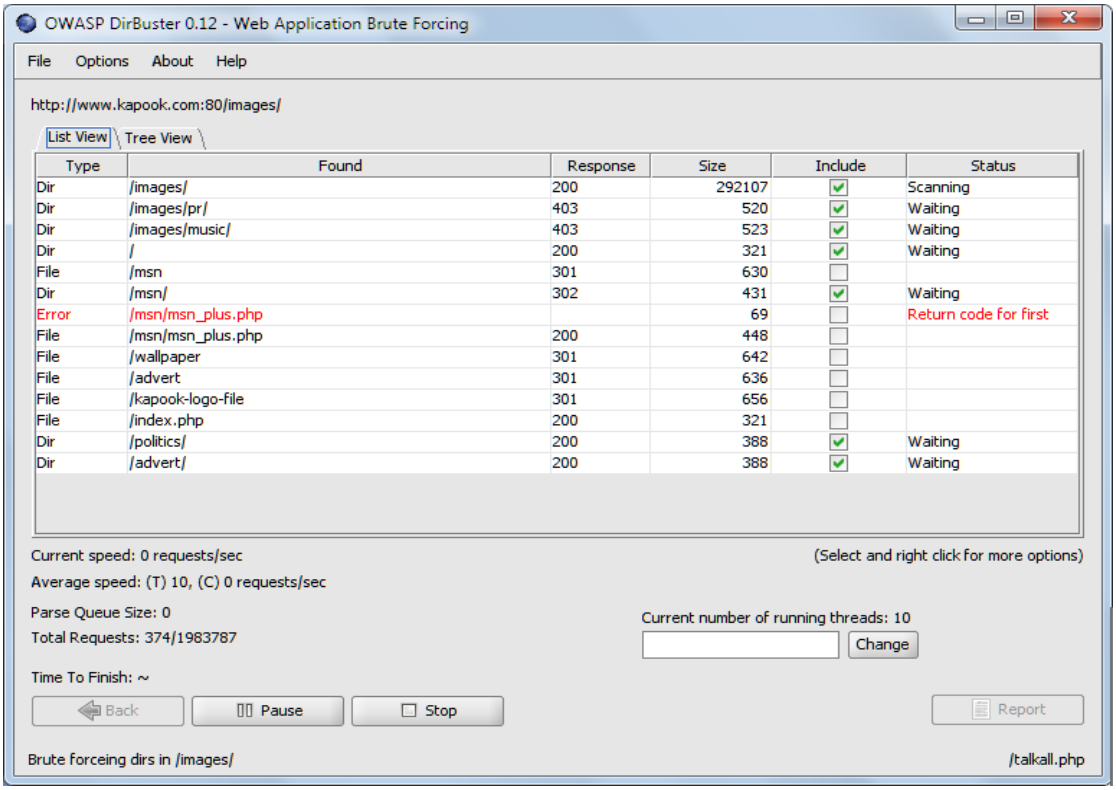
ที่ค้นหาแล้วพบไดเรกทอรี่ /phpmyadmin/ ถ้าฐานข้อมูลนั้นไม่ได้ตั้งค่า username และ password ไว้ก็สามารถเข้าไปดูข้อมูลในฐานข้อมูลนั้นได้เลย



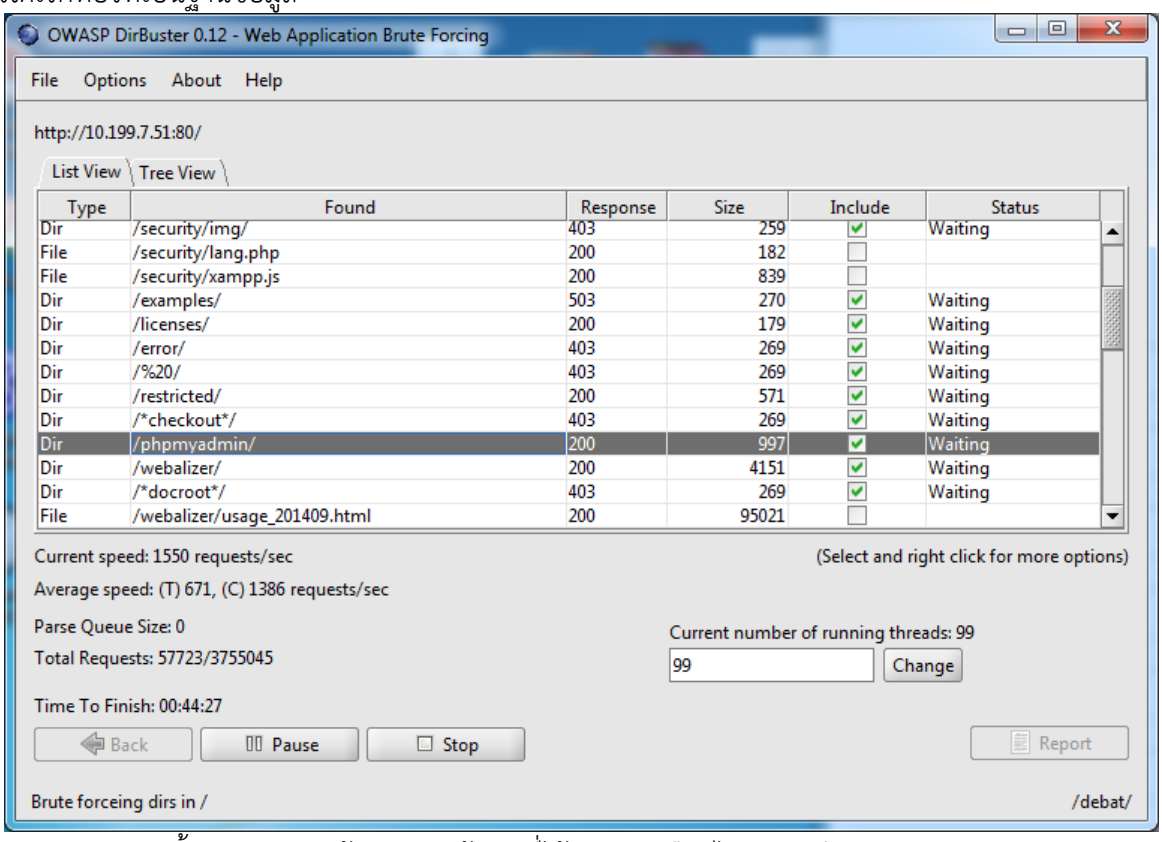
12. ในส่วนของ Dir to start with เป็นการค้นหาไดเรกทอรีเฉพาะที่เราต้องการค้นหา โดยนำชื่อไดเรกทอรีที่เราต้องการค้นหามากรอกใส่ในช่องนี้ได้เลย จากนั้นกดปุ่ม Start เพื่อค้นหาไดเรกทอรีที่เราต้องการ (ตัวอย่างเช่น ต้องการที่จะค้นหาไดเรกทอรีที่มีชื่อว่า /images/)



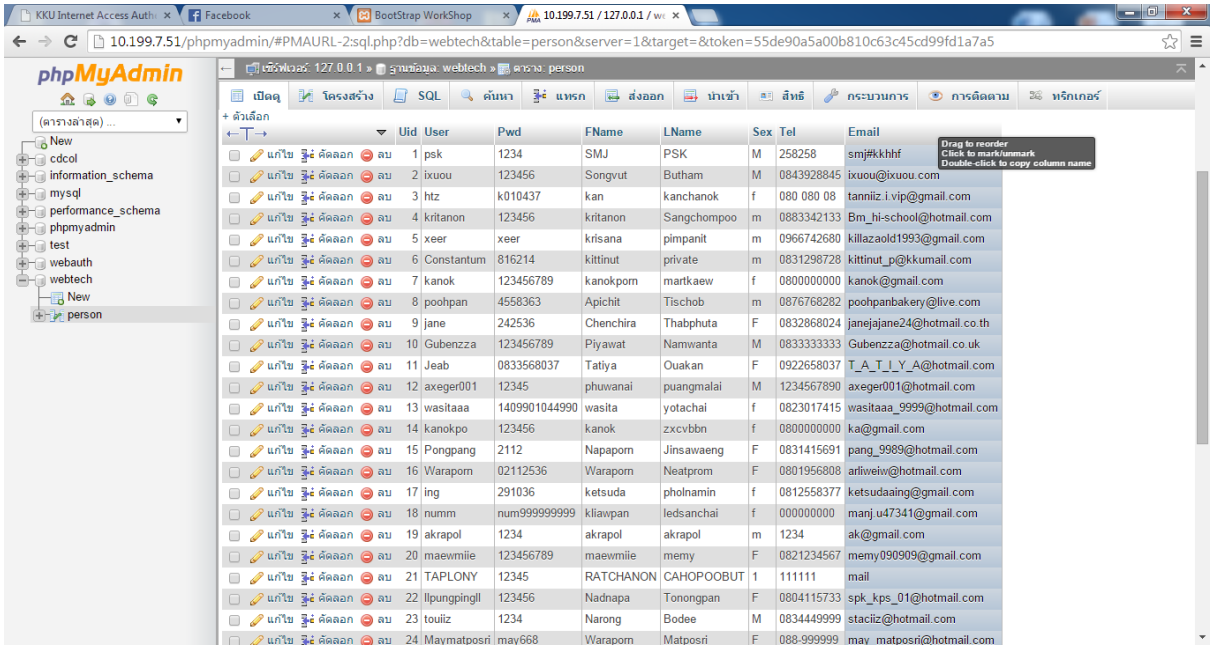
13. โปรแกรมจะทำการค้นหาไฟล์ที่เกี่ยวข้องกับไดเรกทอรีที่ชื่อว่า /images/ ดังรูป



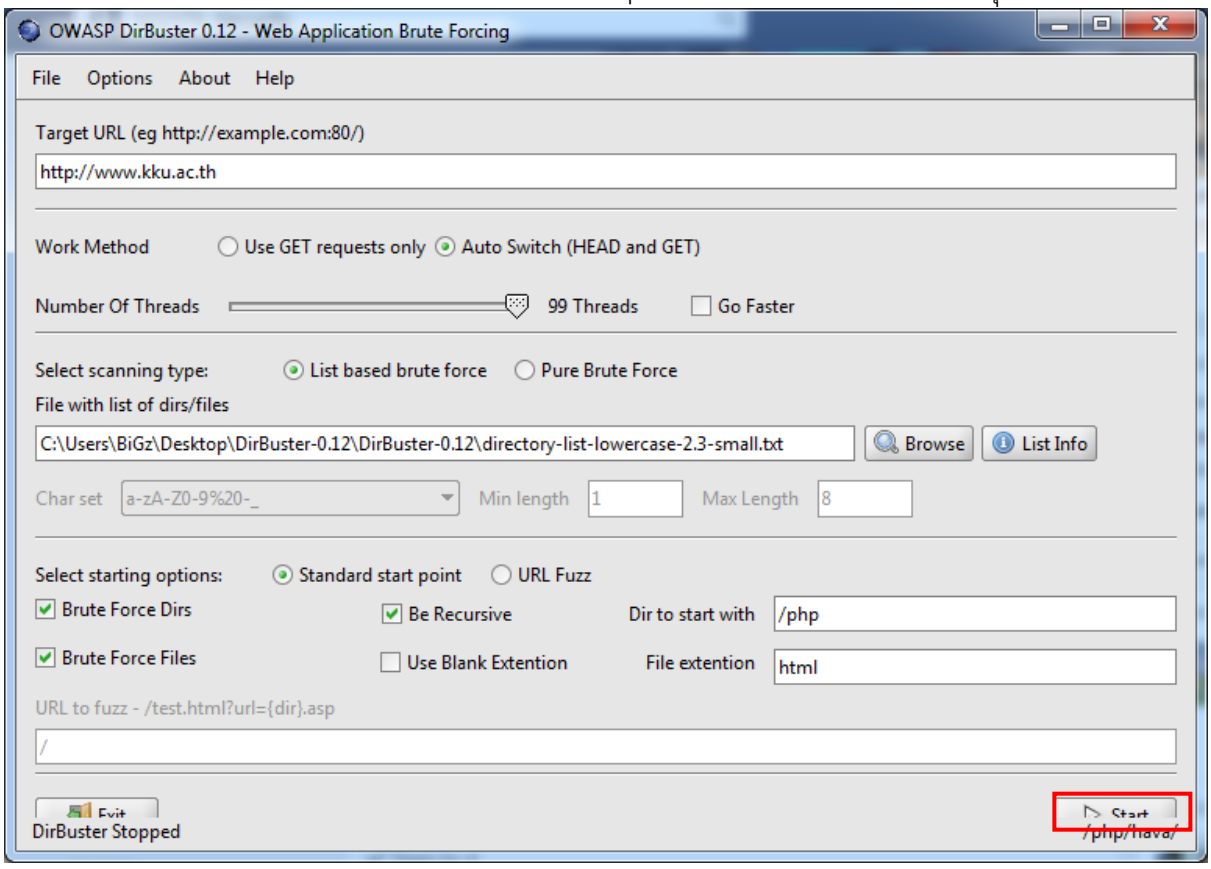
14. ตัวอย่างการค้นหาไฟล์ในไดเรกทอรีของ http://10.199.7.51:80/ และเลือก /phpmyadmin/ ในไดเรกทอรีที่เป็นฐานข้อมูล



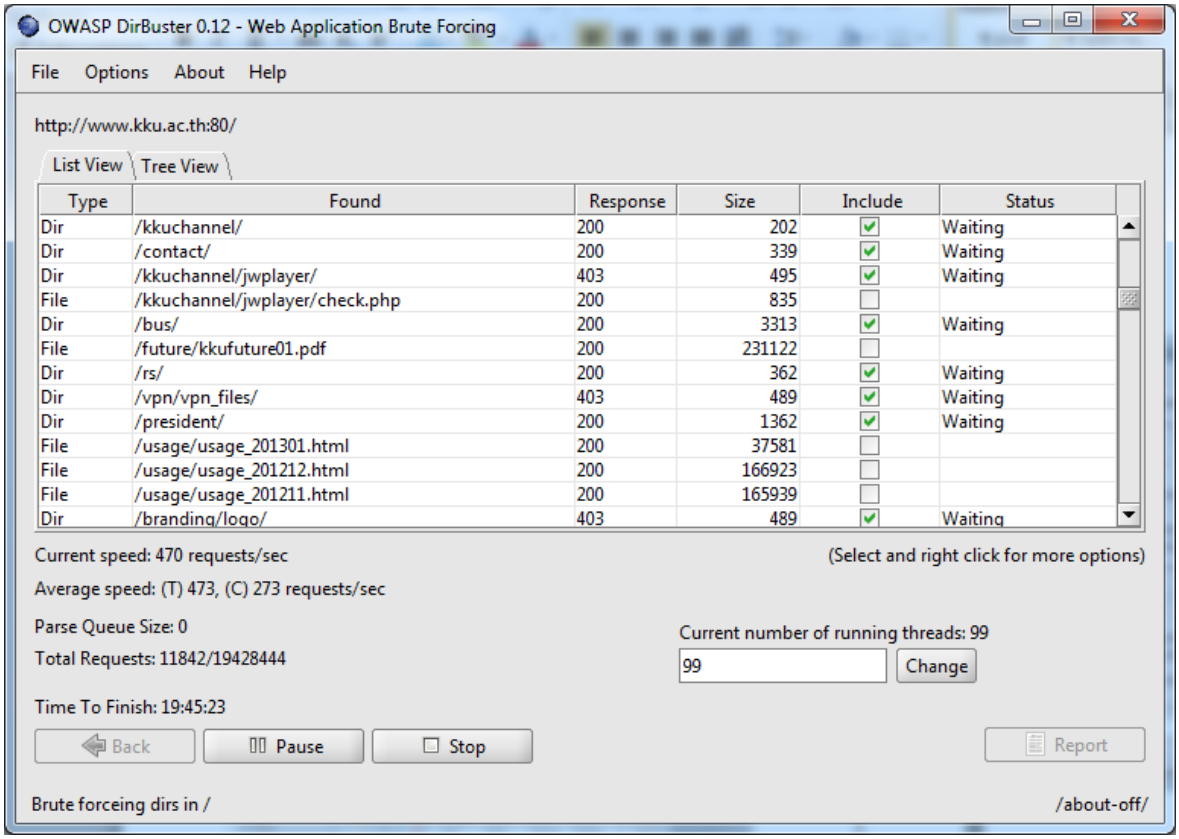
15. จากนั้นจะปรากฏหน้าของฐานข้อมูลที่ได้จากการเลือกไดเรกทอรี /phpmyadmin/



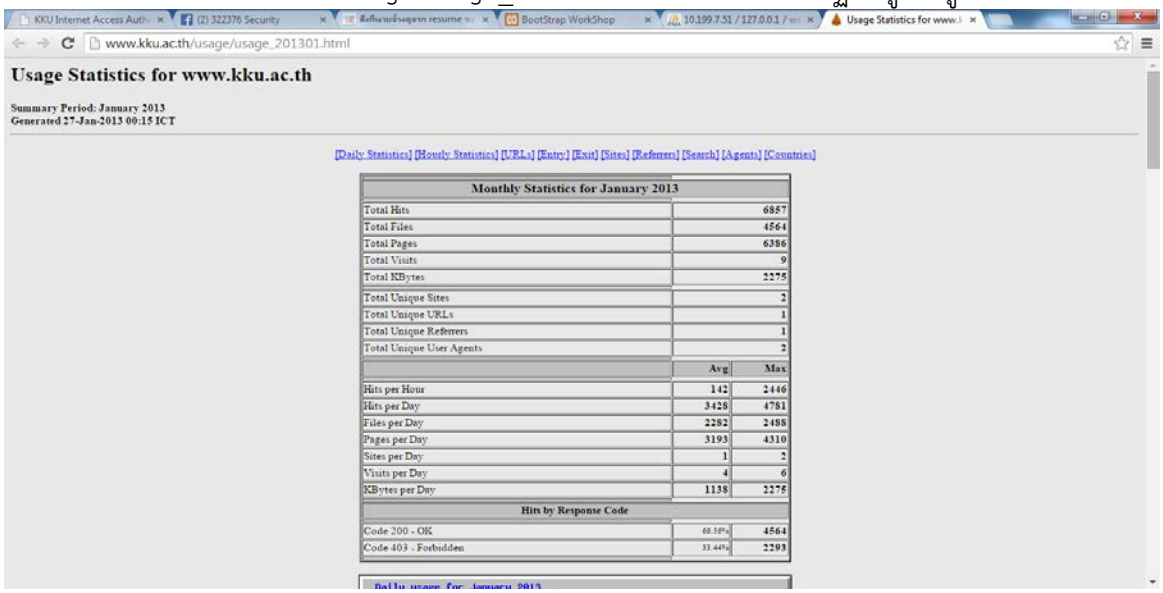
16. ตัวอย่างการค้นหาไฟล์ในไดเรกทอรีของ http://www.kku.ac.th จากนั้นกดปุ่ม Start



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



18. เมื่อกดเลือกที่ไฟล์ /usage/usage_201301.html แล้ว จะปรากฏข้อมูลดังรูป



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=aHCeG4-0olM