

PRACTICAL 07

Problem Statement: Enumerate Webserver using DirBuster

Lab Objectives

In this lab, we will demonstrate how to:

Enumerate a webserver by finding files and directories using DirBuster.

Lab Environment

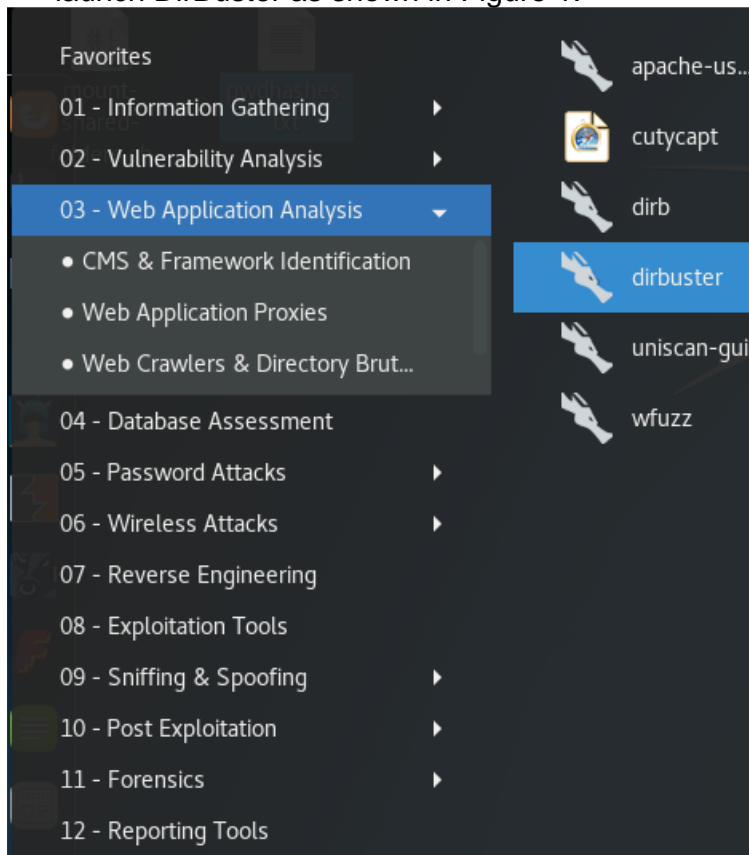
In order to carry out this lab, you will require the following:

1. Administrator privileges
2. Kali Linux machine

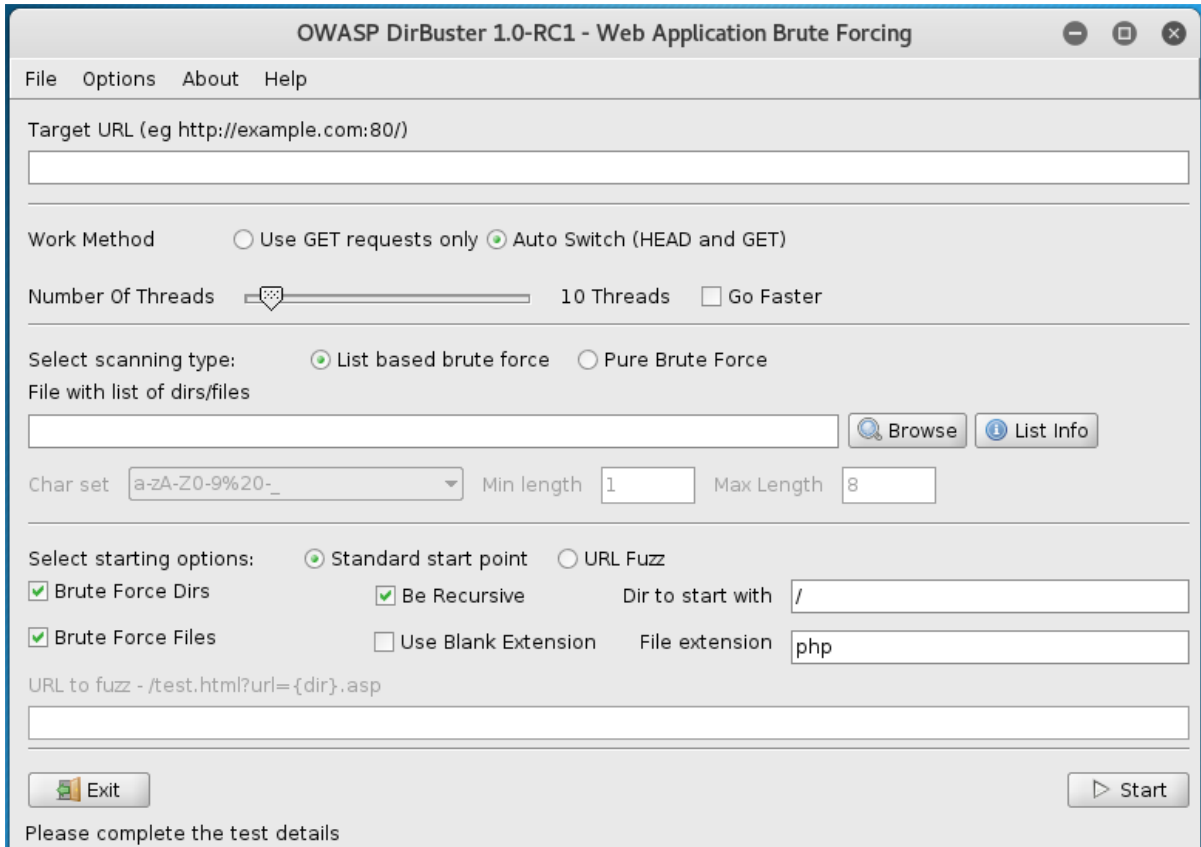
Lab Tasks

To enumerate a webserver by finding files and directories using DirBuster, perform the following steps:

1. Login to Kali Linux machine.
2. Go to Applications -> Kali Linux -> Web Applications -> Web Crawlers -> dirbuster to launch DirBuster as shown in Figure 1.



When it is launched, it opens in a GUI as shown in Figure 2.



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 10 Threads ☐ 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

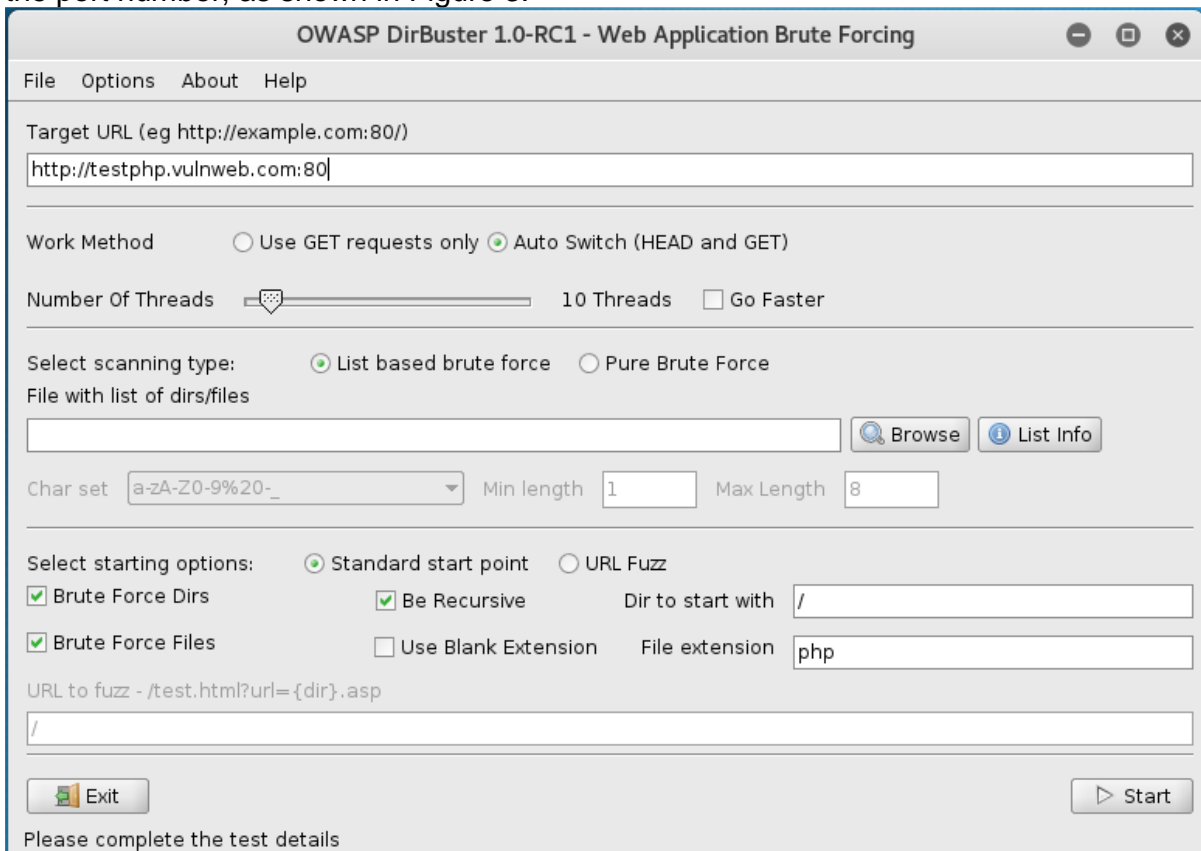
☒ Brute Force Dirs ☒ Be Recursive Dir to start with

☒ Brute Force Files ☐ Use Blank Extension File extension

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

Please complete the test details

3. Type the URL of the website you want to scan in the Target URL text field and the port number, as shown in Figure 3.



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 10 Threads ☐ 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

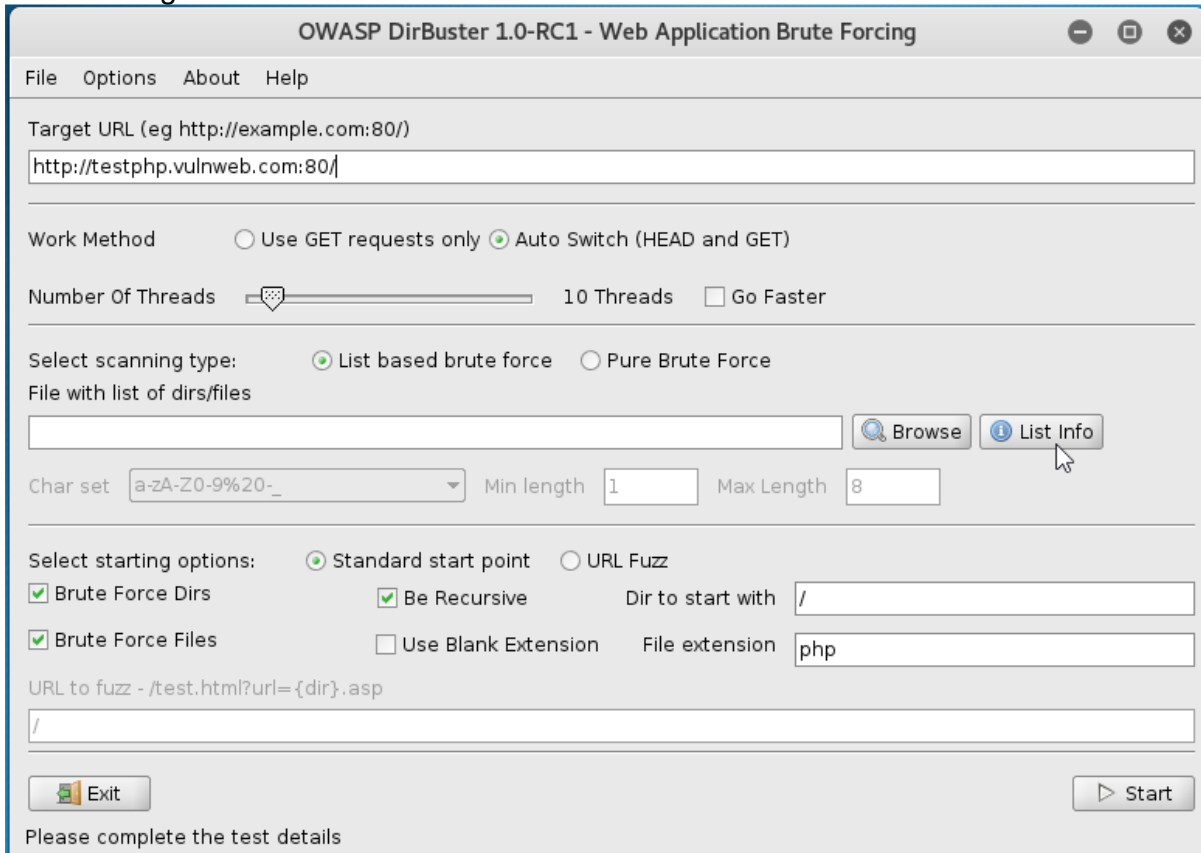
☒ Brute Force Dirs ☒ Be Recursive Dir to start with

☒ Brute Force Files ☐ Use Blank Extension File extension

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

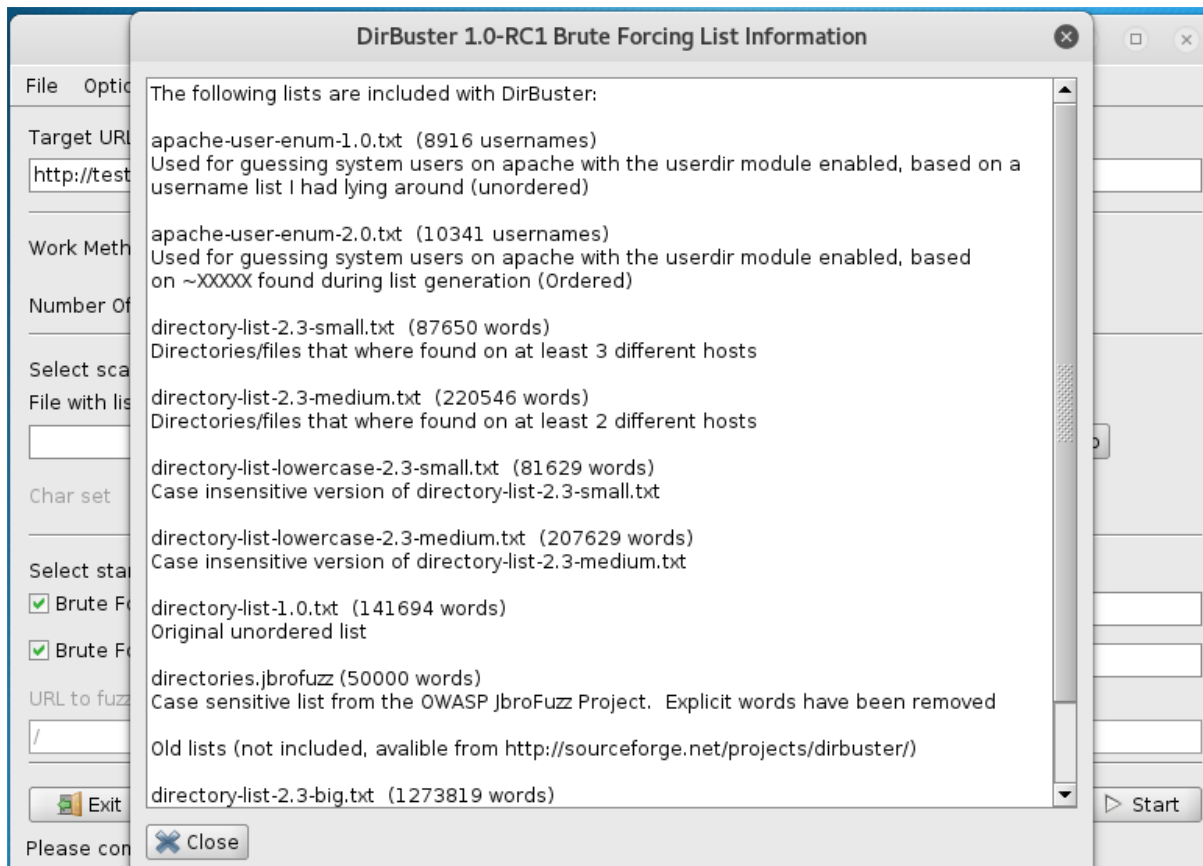
Please complete the test details

4. Click on List Info to open a wordlist to be used to find the directories and files as shown in Figure 4.

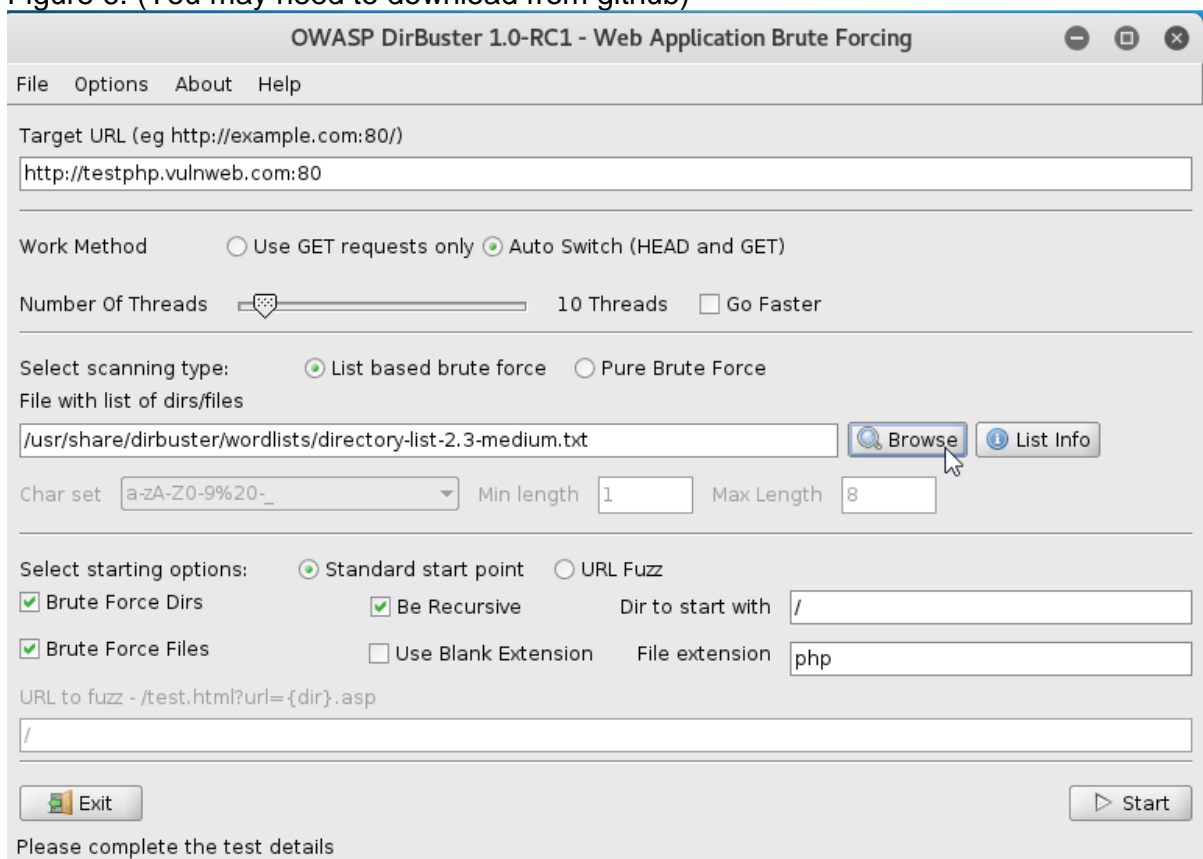


The screenshot shows the OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing application window. The interface includes a menu bar (File, Options, About, Help) and a main configuration area. The Target URL is set to `http://testphp.vulnweb.com:80/`. The Work Method is set to **Auto Switch (HEAD and 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 field is empty, 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 are set to **Standard start point**. The **Brute Force Dirs** checkbox is checked, and the **Be Recursive** checkbox is also checked. The Dir to start with is set to `/`. The **Brute Force Files** checkbox is checked, 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 at the bottom. A message at the bottom says "Please complete the test details".

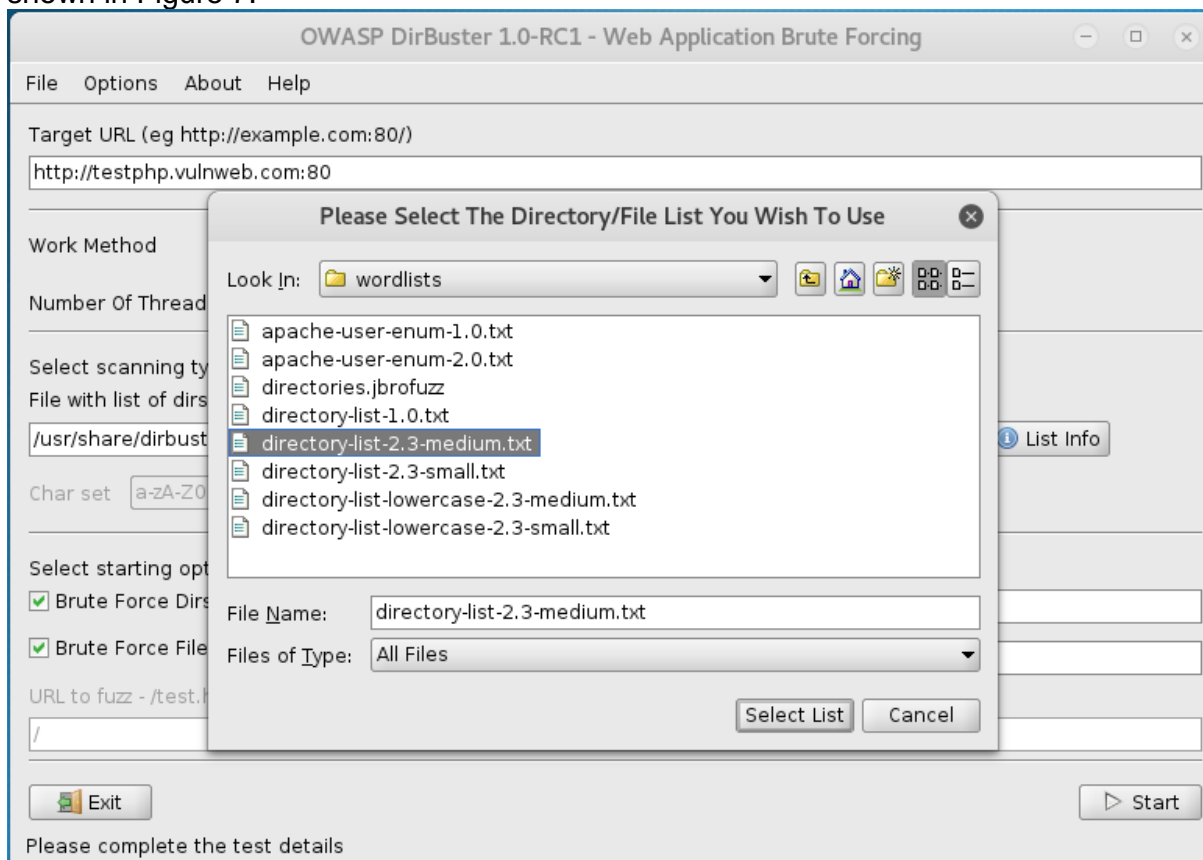
When you click on List Info, it opens a Brute Forcing List Information window listing all the available wordlists with a short description, as shown in Figure 5.



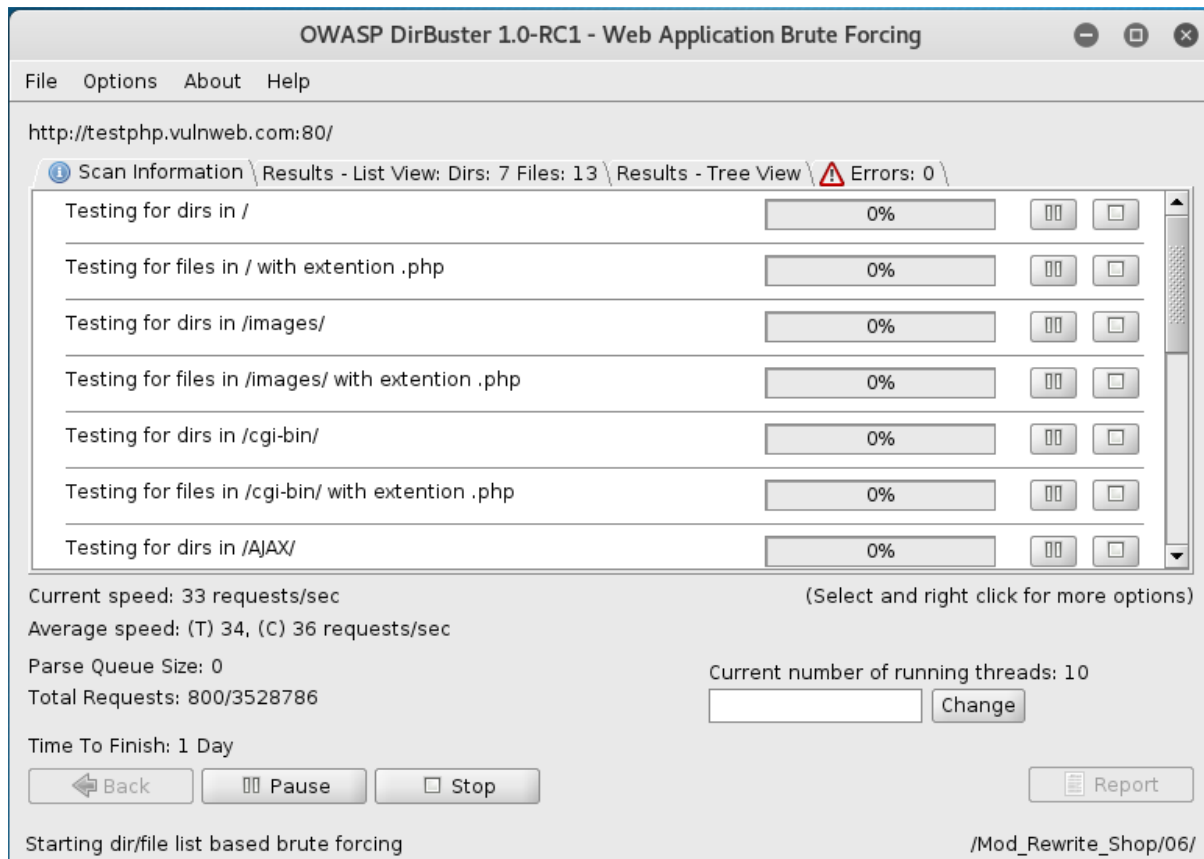
5. Select a list you want to use and click on Browse to open that list, as shown in Figure 6. (You may need to download from github)



6. It will open a Please Select The Directory/File List You Wish To Use window as shown in Figure 7.
7. Browse where your file is saved and select the list by clicking on Select List, as shown in Figure 7.



8. Click on the Start button. When you click on Start, DirBuster starts generating GET requests and sending them to the selected URL with a request for each of the files and directories listed in the wordlist. Figure 8 shows the scan information.



After running DirBuster for some time, you will see the results in Tree View, as shown in Figure 9.

