Dirbuster

DirBuster is a powerful and widely-used web application penetration testing tool designed to discover hidden directories and files on web servers. It operates by performing brute force attacks using wordlists to probe for directories and files that are not easily accessible or indexed. This tool is particularly useful for uncovering sensitive information, misconfigurations, and vulnerabilities that might be hidden within a web application's structure. By efficiently mapping out the directory and file layout of a target web server, DirBuster helps security professionals identify potential entry points and weaknesses that need to be addressed, making it an essential tool in the arsenal of a web application security tester.

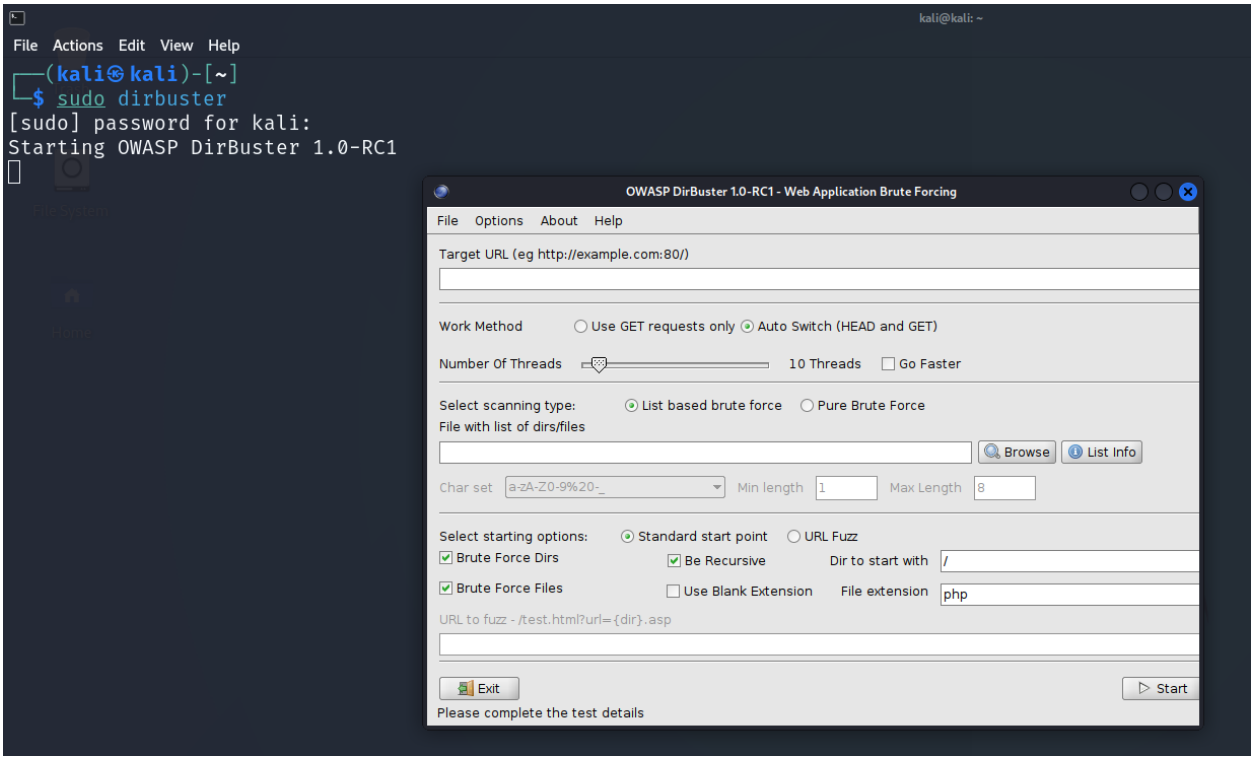
DirBuster is used primarily for web application security testing to discover hidden directories and files on web servers.

- **Identifying Hidden Resources:** DirBuster helps security professionals find directories and files that are not linked or easily accessible from the web interface but may contain sensitive information or functionality.
- **Discovering Configuration Files:** It can locate configuration files that may reveal server settings, database connections, or other critical information that could be exploited.

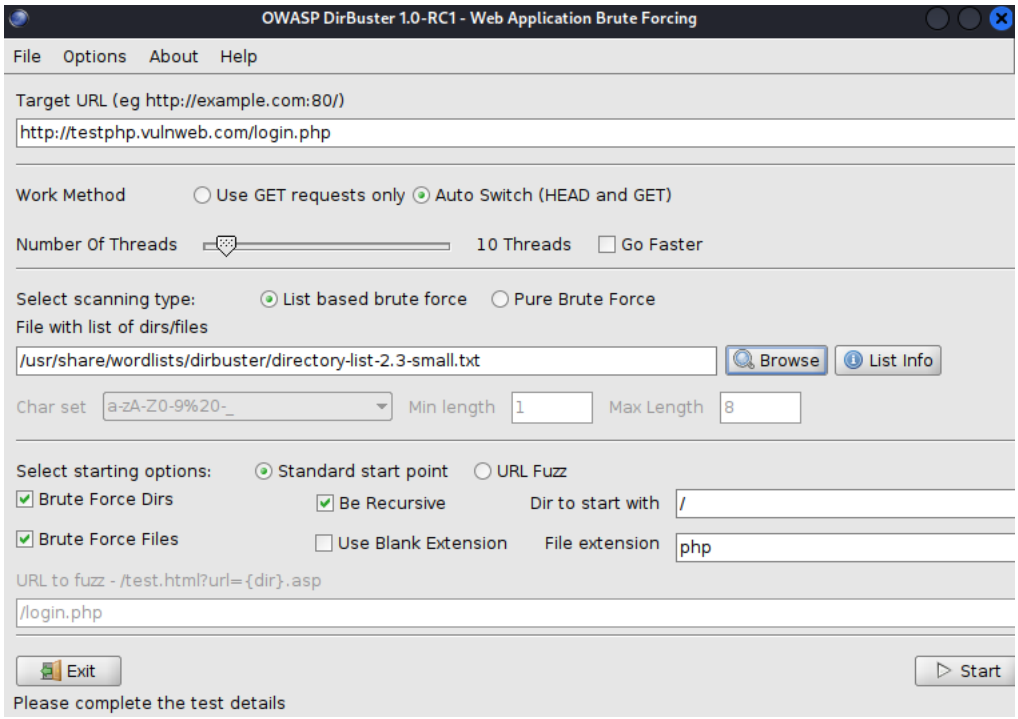
- **Finding Backup Files:** Sometimes, developers leave backup files on the server, which can contain source code or other valuable information. DirBuster can uncover these backups.
- **Exposing Development and Test Files:** Developers often leave development or test files on the production server, which might have vulnerabilities or sensitive information. DirBuster can find these files.
- **Assessing Security Posture:** By mapping out the directory and file structure of a web server, DirBuster helps assess how well a web application is secured and whether there are any overlooked entry points that need to be addressed.

Examples: -

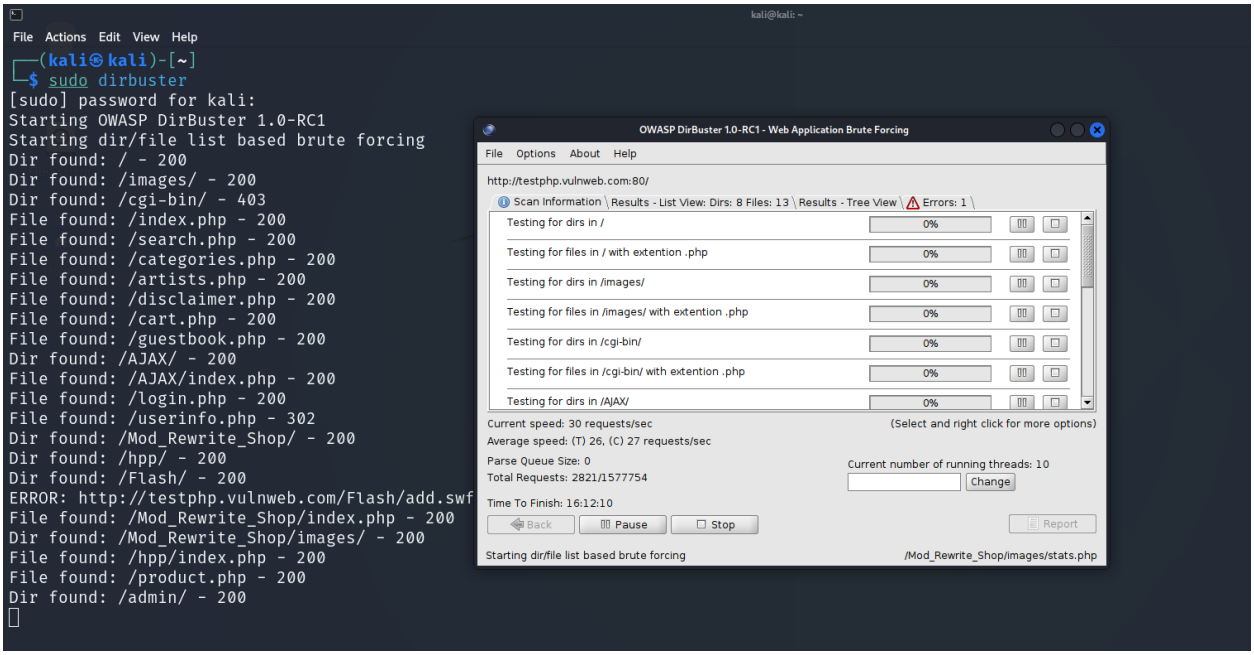
1. First of all, type dirbuster inside the terminal in order to run the too.



2. Now give the target url and the wordlist for the attack. Here we pick default wordlist from linux. The path of that wordlist - /usr/share/wordlist/dirbuster/directory-list-2.3-small.txt



3. After clicking on start we will have the result inside the terminal as you can see below.



4. At the end, we can download the report in text,csv and xml format.