ReadMe

This application was made in Java and named “TheFuzzer”, it was created with the intent of expose vulnerabilities, in this release the application support the following features:

* Discover pages of a given domain;
* Capture all links of pages;
* Capture all forms of pages;
* Capture all inputs of pages;
* Tracks page’s cookies;
* Guess “hidden” pages in the domain;
* Crawl all links containing in the domain’s pages

How to install:

TheFuzzer is a jar file and doesn’t need to be installed, just make sure you have installed the Java JDK in your machine and have fun.

How to use it:

1. Open the Prompt or Terminal
2. To discover pages, links, forms, inputs, cookies, and crawl pages of a domain type the command bellow:

Java –jar PATH discover URL --common-words=com.txt

Arguments Explanation:

Java: command used to invoke java features, required;

-jar: used to run a jar file, required;

PATH: the complete path where the fuzzer jar file is located, required;

Discover: uses the discover features of the fuzzer, required;

URL: the domain of the tested site, required;

--common-words=com.txt: this parameter is required and uses a specified file containing a list of words to “guess” possible pages, required;

Example of the command:

Java –jar discover http://127.0.0.1/dvwa/login.php --common-words=com.txt

Another feature of the Fuzzer that can be used when in sites that require login is the parameter --custom-auth, it is an optional parameter, in this release this feature is available in two domains, they are: DVWA, Bodgeit. To use this feature type the command bellow:

discover http://127.0.0.1/dvwa/login.php --custom-auth=dvwa --common-words=com.txt

OR

discover http://127.0.0.1:8080/bodgeit/ --custom-auth=bodgeit --common-words=com.txt