Computer Security Assignment 7

Venkatesh Viswanathan
50290589

December 7, 2018

1 Question 1

1.1 Mutation Fuzzer using Burp Suite

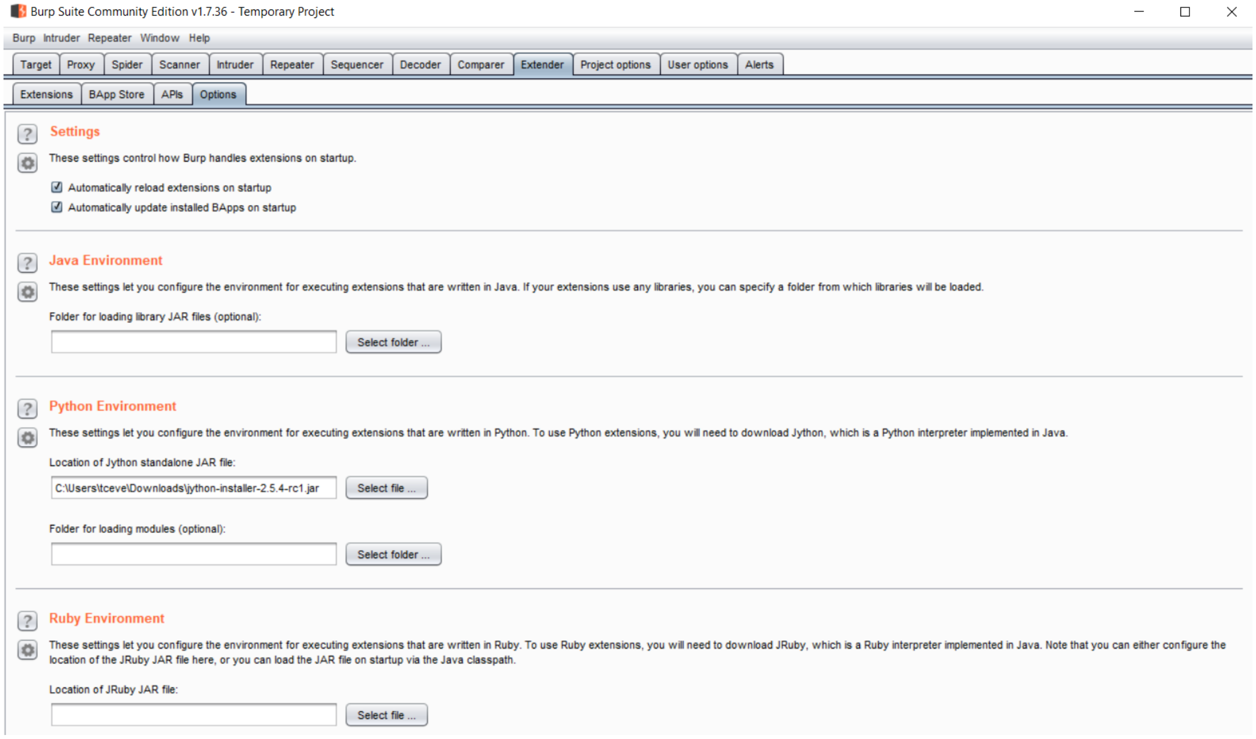
Burp suite is web app analysis tool where you can intercept HTTP/HTTPS requests to carry out attacks, spidering or use other techniques. It is extendable with some tooling features to allow us to introduce our own custom tools.

The goal of this experiment is to mutate the search keywords and produce results rather for the varied keyword. Consider the user has searched for the keyword named "fuzz" and the search results should be as "buzz".This is achieved through using the tool Burp Suite. The main important thing on why i choose to use BURP was that it was the only fuzzing tool in Windows.Most of the other tools are in KALI Linux which i have to run in VM.

Steps to reproduce the Attack

- Before explaining the steps, let me briefly tell about the attack that we are going to perform. For our mutation fuzzer extender, I will use http://testphp.vulnweb.com (a vulnerable website)and make a simple search request on the site.
- This would be intercepted by Burp (which is a proxy listening on localhost:8080) and we should be able to mutate the payloads in that request based on the logic in the python fuzzing extension.
- To accomplish this, we will use 2 reference APIs (you can view them under the APIs tab)
- The first part in reproducing the attack is the installation of the Fuzzing Tool namely the BURP SUITE.This can be installed in BURP SUITE's official link itself.
- The next process is to install JYTHON which allow extenders/ extensions in python.These settings let you configure the environment for executing extensions that are written in Python. To use Python extensions, you will need to download Jython, which is a Python interpreter implemented in Java.

- Upon downloading you will have to give the path in the Extender and then Options tab and give the path for the corresponding JAR file.Burp Suites requires Java to run and described extension reference APIs are all in Java too. A screenshot has been attached below.


Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Extensions BApp Store APIs Options
Select folder ...
Select file ...
Select folder ...
Select file ...

Settings

These settings control how Burp handles extensions on startup.

☑ Automatically reload extensions on startup
☑ Automatically update installed BApps on startup

Java Environment

These settings let you configure the environment for executing extensions that are written in Java. If your extensions use any libraries, you can specify a folder from which libraries will be loaded.

Folder for loading library JAR files (optional):

Python Environment

These settings let you configure the environment for executing extensions that are written in Python. To use Python extensions, you will need to download Jython, which is a Python interpreter implemented in Java.

Location of Jython standalone JAR file: C:\Users\tceve\Downloads\jython-installer-2.5.4-rc1.jar

Folder for loading modules (optional):

Ruby Environment

These settings let you configure the environment for executing extensions that are written in Ruby. To use Ruby extensions, you will need to download JRuby, which is a Ruby interpreter implemented in Java. Note that you can either configure the location of the JRuby JAR file here, or you can load the JAR file on startup via the Java classpath.

Location of JRuby JAR file:

- After importing the jar file into the BURP Suite tool, we will have to add the python code given into the BURP extension like the one shown below.The python code was entirely taken from the link which will be cited at the end of the document.

- The screenshot of adding the python file to the extension is given below.