Software Security 2018

Lab Project : System Security **Summer'18**
Date: 07.06.2018 *Prof. Dr-Ing. Christian Hammer*
Due : 28.06.2018 23:55 *Mohammadreza Ashouri*

Total Points: 10

Submission Instructions:

- Submit the project source code and description file in a compressed file on Moodle. You may write your explanation in TEX. A scanned copy of solutions (in PDF, any other format == rejected) in your own handwriting is sufficient if its legible and taken using a proper scanner. ***It's your responsibility to make the scanned copy legible.*** *Illegible copies will not be evaluated.*
- Submission deadline is **28.06.2018 23:55**.

1 Project Description

The main aim of the project is to assess your understanding of the vulnerabilities such as stack overflow and format string. Consequently, you must be able to build a basic fuzzing tool for diagnosing the overflow related vulnerabilities on a given program.
Your tool must include the following features:

1- Detecting of overflow vulnerability on a given program. For example:

```
$ Root@local: ./tool vuln.o AAAAA.... -> segment fault!
```

2- Detecting of format string on a given program. For instance:

```
$ Root@local: ./vuln.o AAAA%X%X%X...
```

An example of how your tool should look like:

```
$ Root@local: your_tool program_name [vulnerability type]
EX:
  Root@local: /tool vuln.o OVERFLOW
  Root@local: /tool vuln.o FORMATSTRING
```

When the tool catches a vulnerability, for example, a segmentation fault error,then it must display the result in ***terminal*** or saves the result in a plain text file, for example, ***report.txt***.

2 Disclaimer

The information provided is to be used for educational purposes only. The author is in no way responsible for any misuse of the information provided.