IT-Security 2017

Exercises: Software Security

Due date: 24. November 2017
Notice: If you use any self-developed programs or tools for the exercises, also hand in the complete source code and a short documentation. Also, state how you solved the problem. Clearly state literatur you used to solve the exercises and include a link, screenshot or any other form of documentation for all of your sources. If you split the exercises and not all team members solve all the exercises, state this at the beginning of your answer.

Attention: Exercises 1-3 have to be solved without changing the source code! You are supposed to use the program in the provided way and exploit vulnerabilites in the programs.

Exercise 1: Circumventing weak security checks

In `exercise1.c` you will find an implementation for a chemical factory control software. The program can be used to increment or decrement certain ingredient of the factory. The program implements security checks to prevent this, but these checks can be circumvented. Your goal is to find a way to decrease values below 0 and increase values above 1000. Also provide possible solutions to disable these bypasses.

Weblink:
https://www.dropbox.com/sh/9foqer11fdzzwhx/AACZ27TwsA94xd5cWXpICW7va?dl=0
Usage: `gcc exercise1.c -o exercise1.o && ./exercise1.o`

Exercise 2: Changing strings without directly accessing it

In `exercise2.c` you will find a program that asks a user for her or his name and prints another string afterwards. Your goal is to find a way to change the displayed string to say "exercise succeeded". Again, provide possible strategies to disable the security bypass **and** name the technique used to exploit the program.

Weblink:
https://www.dropbox.com/sh/9foqer11fdzzwhx/AACZ27TwsA94xd5cWXpICW7v

a?dl=0
Usage: `gcc exercise2.c -o exercise2.o && ./exercise2.o`

Exercise 3: Gaining access to restricted files

`exercise3.c` is designed to check whether you you try to access `secret_file.txt` or a symbolic link to this file. You are supposed to find a way to access the file `secret_file.txt` via the `exercise3.o` program even though the security check tries to prevent this. Give a strategy on how to disable the security bypass.

Weblink:
https://www.dropbox.com/sh/9foqer11fdzzwhx/AACZ27TwsA94xd5cWXpICW7va?dl=0
Usage: `create_exercise.sh && gcc exercise3.c -o && ./exercise3.o`

Exercise 4: Software Security in Practise

Explain the exploit as well as the impact of the so called *Heartbleed* security bug **in your own words**. Also try to find an explanation why it has been undetected for so long and how it was finally fixed. Remember to make reference of all sources you use from the internet for your research.