TP Class Assignment - - 27/05/2019

These exercises are optional.

Note: Save the files in the directory Aula 13 to your local machine in the directory /home/user/Classes/Class 13 (suggestion, if you are using the virtual machine).

Exercises

1. Input validation

Experience 1.1

Analyze the InputValidation.cpp and InputValidation.java files.

1. Explain the two problems: (i) usage of cin/Scanner for reading, (ii) accessing the array
2. What would you change?

Experience 1.2

Analyze the file WhileEx.java.

1. What are the problems with the program input?
2. Change the program to validate all the input and recover gracefully from the errors.

Experience 1.3

Analyze the file Input.cpp.

1. What are the problems with the program input?
2. Change the program to validate all the input and recover gracefully from the errors.

Experience 1.4

Analyze the file Input.java.

1. What are the problems with the program input?
2. Change the program to validate all the input and recover gracefully from the errors.

Experience 1.5

Analyze the program filetype.c that prints on the screen the file type of the argument (file path).

1. There are at least two types of vulnerabilities studied in the theoretical "Input Validation" class that can be exploited. Identify them.

2. Provide the code/steps/command line that allow to exploit each of the vulnerabilities identified in the previous question.

3. What would happen if your program had *setuid root* permissions?

Experience 1.6

Analyze the program readfile.c that prints on the screen the contents of the filename passed as an argument - the suffix ".txt" is added to the filename to ensure that it only lets you read text files.

1. There is a vulnerability studied in the theoretical "Input Validation" class (in conjunction with another that you have already studied) that allows the program to print files that do not end in ".txt". Explain.

2. Enter the command line required to access the */etc/passwd* file.

Experience 1.7

Analyze the file string_format.c with the format string vulnerability sample explained in the theoretical class, and the string_format2.c file without the vulnerability.

1. Experiment with multiple input values with both the vulnerable and the non-vulnerable program and draw your conclusions.

2. Principles of software design

Experience 2.1

Consider the principles of software design studied in the theoretical class, and justify which of the principles are not followed in each of the following situations:

- A company that produces security-related components does not disclose details about the design of the components, allegedly for "security reasons";
- An application downloads code from the Internet and starts executing it without asking the user if he wants to start executing the code.