IT-Security 2019

Exercises: Software Security

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 increm ent or decrem ent certain ingredient of the factory. Your goal is to find a way to decrease values below 0 and increase values above 1000. The program implements security checks to prevent this, but these checks can be circumvented. Also provide possible solutions to disable these bypasses.

Weblink: http://bit.ly/itsec-w4-e1

Usage: `gcc exercise1.c -o exercise1.o && ./exercise1.o`

Exercise 2: Changing a variable 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 goalis to find a w ay to change the displayed string to say "exercise succeeded". Again, provide possible strategies to disable the security bypass and nam e the technique used to exploit the program.

Weblink: http://bit.ly/itsec-w4-e1

Usage: `gcc exercise2.c -w -o exercise2.o && ./exercise2.o`

Exercise 3: Gaining access to restricted files

exercise3.c is designed to check w hether you you try to access *secret_file.txt* or a symbolic link to this file. You are supposed to find a w ay 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: http://bit.ly/itsec-w4-e1

Usage: `echo 42 > secret_file.txt && gcc exercise3.c -w -o exercise3.o && ./exercise3.o`

Exercise 4: Time Traveler - Getting sensitive information from internal files

The URL given below leads you to a website hosted by a time travelling software developer. The website used to show the upcoming lottery numbers. However, the creator eventually decided to remove the numbers from the website, so they can not be seen anymore.

Tip: The host of the w ebsite seem s to be using *Git* as its serving a suspicious folder at */git*.

1. **Find out the lottery num bers that used to be in *index.html* and explain the steps you perform ed to reveal them.**
2. **What are your advises to developers to prevent such a hack from happening in the future.**

Weblink: http://bit.ly/itsec-w4-e1

Exercise 5: Software Security in Practise

Explain the exploit as w ellas the im pact of the so-called *Heartbleed* security bug in your own words. Also try to find an explanation w hy it has been undetected for so long and how it was finally fixed.

Reminder: Always cite all your sources!

Exercise 6: Software Scanning Tools

In this course you've learned about a variety of potentialrisks in softw are code that m ay not be visible at first glance. Softw are scanning tools support you in continuously detecting such risks before your code reaches production.

Perform a scan w ith a static softw are scanning toolof your choice (e.g., *SonarQube*) on a publicly hosted software project and attach the report to your submission.