UP24 Lab04

Date: 2024-05-06

Race & Reentrant + Homework #2

This lab aims to investigate possible race or reentrant errors from multithreaded programs. Please read the codes and solve the challenges available on the two challenge servers.

Also, as we introduced in our last lecture, we allocate a few points for the assembly challenges you may have already solved in the past week.

Challenge #1

The challenge server #1 can be accessed using the command:

```
nc up.zoolab.org 10931
```

Once you have connected to the challenge server, please dump the content of the `flag` file on the server.

We provide the source code of the challenge server for your reference [view (https://up.zoolab.org/code.html?file=unixprog/lab04/unixfortune.c)].

Challenge #2

The challenge server #2 can be accessed using the command:

```
nc up.zoolab.org 10932
```

Once you have connected to the challenge server, please ask the challenge server to retrieve the secret from localhost:10000.

We provide the source code of the challenge server for your reference [view (https://up.zoolab.org/code.html?file=unixprog/lab04/flagsrv.cpp)].

Homework #2

As we announced in the last lecture, we have created a few assembly challenges for you to practice implementing assembly codes. The scores for HW2 and Lab4 are calculated independently. However, you can choose to demo up to 6 challenges listed in HW2 CTFd to earn 30 points in Lab4. (5 pts per challenge, up to 6 challenges).

See the detail for HW2 in the section.

Lab Grading

1. [20 pts] You can solve challenge #1.

2. [15 pts] You can solve challenge #1 using a `pwntools` script.

3. [20 pts] You can solve challenge #2.

4. [15 pts] You can solve challenge #2 using a `pwntools` script.

5. [30 pts] Solve 6 assembly challenges, each worth 5 pts.

Lab Submission

You have to upload all your solution scripts and codes to e3. Specifically, grading item #2, #4, and #5.

- Filename: `{studentID}_lab04.zip`
- Format:

```
+---{studentID}_lab04
|    chal_1.py
|    chal_2.py
|    {#num}.s
|    other files...
```

You need to put your files in a directory first, then compress the directory.

UP24 HW2

- The challenges are listed in CTFd (updated) (https://up-ctf2.zoolab.org/). (23 challenges)
- You can login to the platform using the username and password we provided.
- You have to submit your flags to CTFd, or you will get no points for this homework.
- We will calculate your grade based on your score on the CTFd scoreboard after the deadline.

Homework Grading

In CTFd, there are a total of 230 points. Your score for this homework is calculated linearly, meaning that it is determined based on the following formula:

$$(yourpoints \div 230) \times 100$$

Homework Submission

You need to submit all your codes `{#num}.s` to e3. The `#num` for each challenge is the last two digits of the challenge port.

- Due date: 2024-05-14 23:59 (updated)
- Filename: `{studentID}_hw2.zip`
- Format:

```
+---{studentID}_hw2
|    00.s
|    01.s
|    02.s
|    ...
|    (or your python script, sol.py)
```