**CSE 5474 — Software Security** Spring 2022

# CTF Writeups

*Week 2 Warmup CTF* *Hezhuang Tian*

## 1 Overview

In CTF1, we have four warm up questions to practice. The difficulty level are increasing as the level up. Generally speaking, using ghidra to analyze and observe source codes of four binary files is the method of doing CTF1.

General Steps:

1. type **file <filename>** to check what the file type is(Although it is given by the CTF1 description, checking file type is a good starting point).
2. type **strings <filename>** to check if there's any obvious hint.
3. import binary file to ghidra and analyze its source code.
4. write down requirements of the password.
5. solve the password.

## 2 Steps of how to Solve the Challenges

### 2.1 Level 1

In level1 warm up, I simply use **strings** command. Then I found a string that looks like password next to "Congratulations! You win"

### 2.2 Level 2

In level2 warm up, the situation is a bit harder than level1.We cannot simply guess the password from **strings** or commands like **angr**. Then I import the binary file to ghidra and try to find some hints from source code. I noticed that the source code use a sequence of conditional statement to check if the password is correct. Finally, I found the correct password by combining characters of conditional statements.

### 2.3 Level 3

In level3 warm up, we have to analyze main function and check_password function. The final password should be equal to 0xaf0b90(11471760 in decimal). The check_password function adds two password together. Hence the password will be a+b = 11471760, if a is the first password and b is the second password. I chose a = 11471759 b = 1 as the passwords.

## 2.4 Level 4

After analyzing the binary file, I found that the final password should be equal to 0xfe6124(16671012 in decimal). Moerover, the final password consists of four separate password. If a,b,c,d are the four passwords, we have:

$$a < 1, b < 1, a * b > 11$$

$$c\%d = 0, c * d = 16671012$$

In order to fulfill the password's requirement, I chose password4: -3 -4 8335506 2 as the values of a,b,c,d. The password4 is correct.