**CSE 5474 — Software Security** Spring 2022

# CTF6 Writeups

*heap CTF* *Tron Tian*

## 1 Overview

In CTF 6, we comprise shells by exploiting heap vulnerability in the programs.The methods provided by the ctf hints are extremely useful for solving the heap challenges.

## 2 CTF Write-ups

### 2.1 Level 1

In this challenge, we need to edit chunks with value of DEADBEEF. First, we add two chunks of data which will be deleted later. After deleting the chuncks, we edit previous chunk with check_varaible address 0x6020F0. Then, we add two chunks of data. Finally we edit the former chunk with value of DEADBEEF

### 2.2 Level 2

Challenge 2 is similar to challenge1. However, this time we add chunks and free chunks twice. We directly add chunks with expected value twice to overwrite check_variable.

### 2.3 Level 3

In challenge 3, we need to use exit() function to locate the GOT table. First we add two chunks and free them.. Then we add a chunks with values of address of the win() function.

### 2.4 Level 4

Challenge 4 is similar to challenge3. However, we add two chunks simultaneously before add chunks with value of win() function's address.

### 2.5 Level 5

In challenge 5, since we need to perform heap operation three times, I assembled the process of allocating and freeing chunks as a method named dword_shoot(The detail of the function can be found by searching dword_shoot on google). Then we activate the dword_shoot function three times to capture the flag.

### 2.6 Level 6

In challenge6, I modified scaffolding methods to make it easier to use. After leaking libc address, we add two chunks with bin/sh then free them. Finally, we add chunks with value of our payload to replace the libc.

### 2.7 Level 7

Challenge 7 is similar to challenge 6. We first get libc adrees then allocate chunks with value of bin/sh. After replacing the GOT table with setuid as the last entry, we comprised the shell to capture the flag.

### 2.8 Level 8

In challenge 8, the hardest part is to find the address of libc. After leaking address of libc, we attack fast bins to comprise it to point at GOT table. Then we replace the GOT table as what we did in previous challenges.

### 2.9 Level 9

The attacking routine of challenge 9 is pretty similar to challenge8. However we need to take care of where chunks we are allocating.