DESCRIPTION

Someone has tampered with the executable file. Please fix it! The fixed binary should give you the flag when you run it.

RESOURCES

As part of the challenge I received an executable file called **call_main** as an attachment for analysis.

APPROACHES

1. The first trial I had was to directly run the executable and I ended up with an: **Hello World** message.

```
mihnea@HOME-PC:/mnt/c/Users/mblot/Desktop/CNS$ ./call_main
Hello, there!
```

2. Then, I directly decompiled the executable using Ghidra and looked into the main function:

```
undefined8 main(void)

{
  decrypt_flag(DAT_00601040,7);
  if (DAT_00601048 == 0x5f534e43) {
    puts((char *)&DAT_00601048);
  }
  else {
    puts("You managed to call me in a wrong way. Try again");
  }
  return 0;
}
```

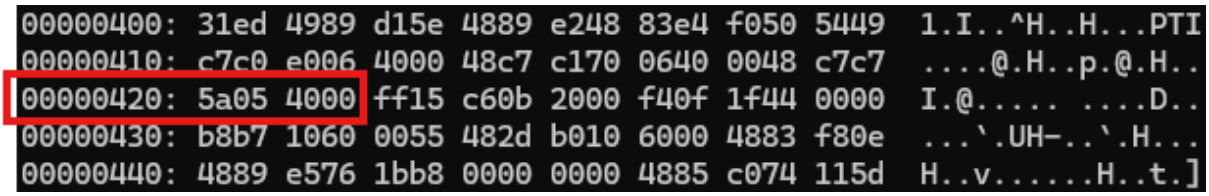
3. The implementation of the main function compared with the fact that I received a: **Hello World** output made me think that it has nothing to do with the main function as there is no possibility of printing **Hello World** from here. This aspect and the fact that **main** is normally the first visible function that gets executed made me think that we never actually end up executing **main**, so I checked the **_start** function that should be called before calling **main**.

```
void processEntry _start(undefined8 param_1,undefined8 param_2)

{
  undefined auStack_8 [8];

  __libc_start_main(dummy,param_2,&stack0x00000008,__libc_csu_init,__libc_csu_fini,param_1,auStack_8
                    );
  do {
                     /* WARNING: Do nothing block with infinite loop */
  } while( true );
}
```

4. Here I noticed that **_start** function calles **_libc_start_main** function with the first parameter as **dummy** which indeed was just **a function that printed Hello World**. Thus, What I had to do is that I entered the executable with **VIM** to edit it and make **_libc_start_main** be called with the first parameter as **main**.



5. After this change from **0x00400549** to the address of main which is **0x0040055a**. I ran the executable and I got the following flag:

CNS_CTF{They're_coming_to_take_me_away_ha_ha}

6. I included in the ZIP the already modified **call_main** file that now has just to be ran in order to obtain the flag.