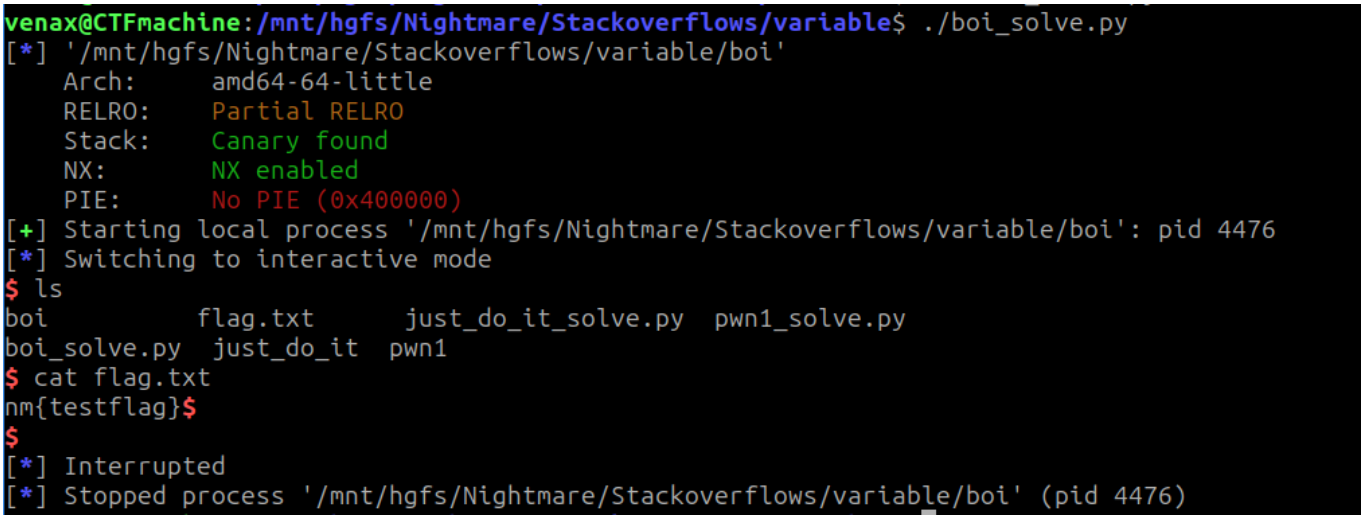
Stack overflows (Variable)

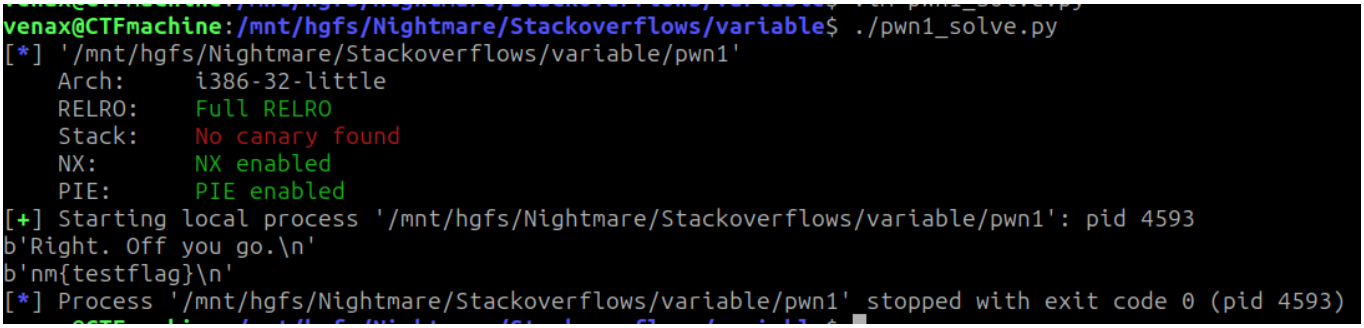
Csaw 2018 Quals: Boi

This one is fairly simple, all you have to do is overwrite the int value with `0xcafebaee`. Doing that, I get the flag



TAMU'19: Pwn1

There's hardcoded string answers to the first two question which can be found by reversing the binary. The third one takes in an input where we overwrite a hardcoded local variable with the value that is expected (`-0x215eef38`). On doing that, we get the flage.



TokyoWesterns'17: JustDoIt

The flag is read from a file into a static variable in memory.

```
pcVar1 = fgets(flag,0x30,local_18);
if (pcVar1 == (char *)0x0) {
  perror("file read error.\n");
                    /* WARNING: Subroutine does not return */
  exit(0);
}
puts("Welcome my secret service. Do you know the password?");
puts("Input the password.");
pcVar1 = fgets(local_28,0x20,stdin);
if (pcVar1 == (char *)0x0) {
  perror("input error.\n");
                    /* WARNING: Subroutine does not return */
  exit(0);
}
iVar2 = strcmp(local_28,PASSWORD);
if (iVar2 == 0) {
  local_14 = success_message;
}
puts(local_14);
return 0;
```

At the end there is a `puts` call to print the success message, so we just have to overwrite the address of local_14 with the address of the static variable `flag`.

```
venax@CTFmachine:/mnt/hgfs/Nightmare/Stackoverflows/variable$ ./just_do_it_solve.py
[*] '/mnt/hgfs/Nightmare/Stackoverflows/variable/just_do_it'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x8048000)
[+] Starting local process '/mnt/hgfs/Nightmare/Stackoverflows/variable/just_do_it': pid 4803
[+] Receiving all data: Done (13B)
[*] Process '/mnt/hgfs/Nightmare/Stackoverflows/variable/just_do_it' stopped with exit code 0 (pid 4803)
nm{testflag}
```