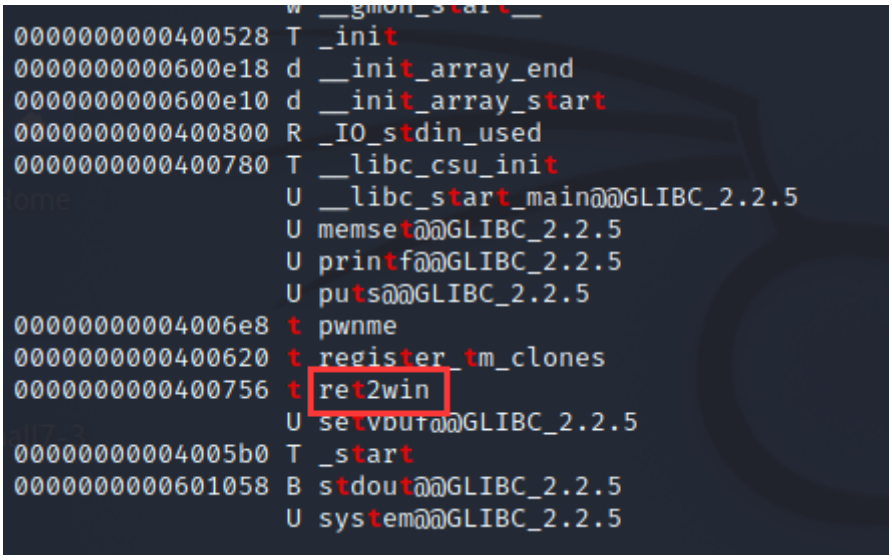
ctf12

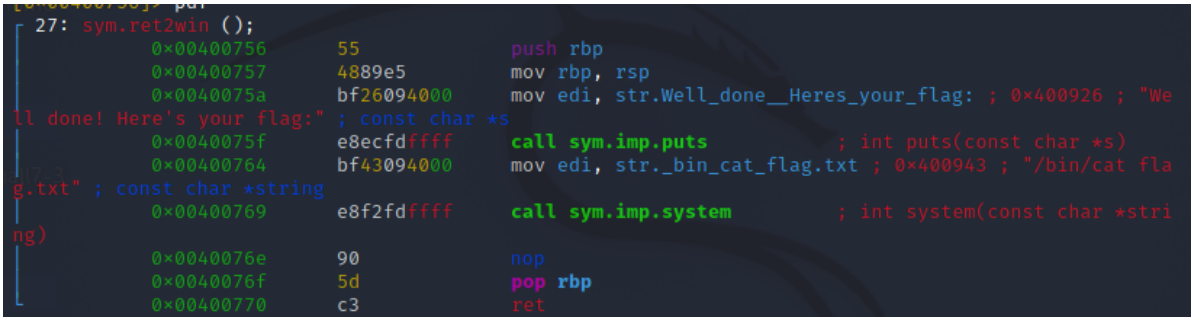
task2

```
nm ret2win|grep ' t '
```



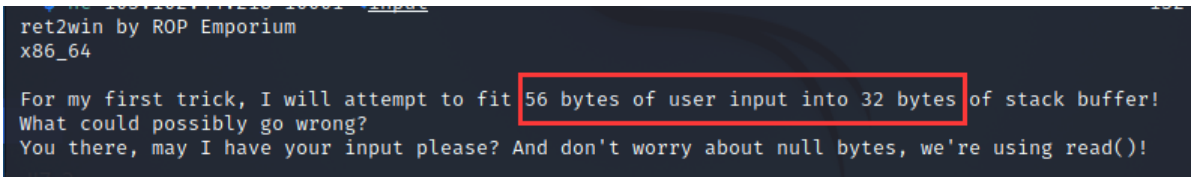
radare check assembly code of ret2win

```
$ radare ret2win
$ aaa
$ afl
$ s sym.ret2win
$ pdf
```



And I find the address for ret2win is **0x00400756.**

Find a buffer flow here.

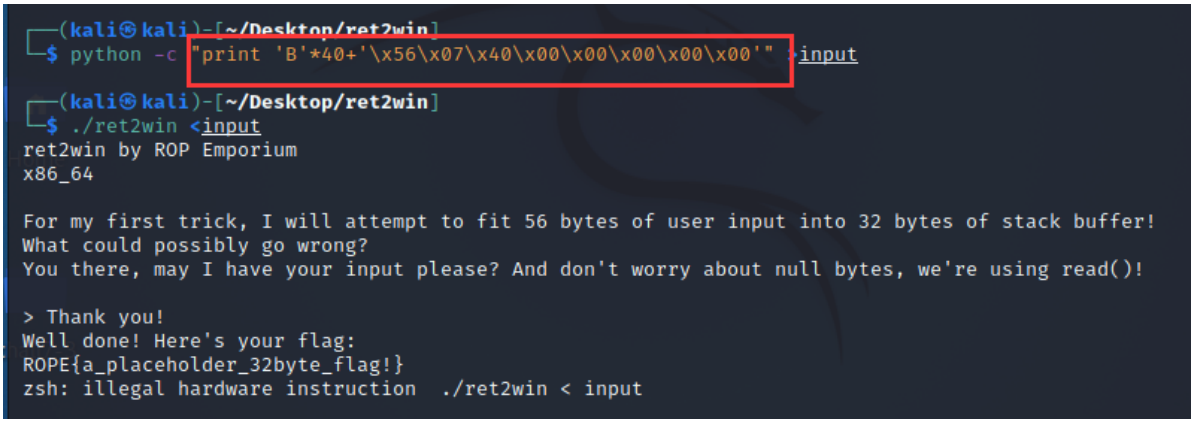


And by trying I find the address is 16 bit like this

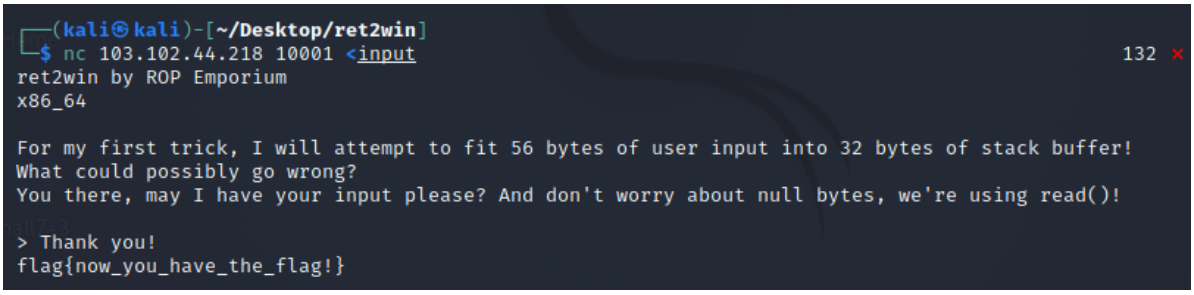
So I should fully overwrite it.

The result is as follows:

In the local :

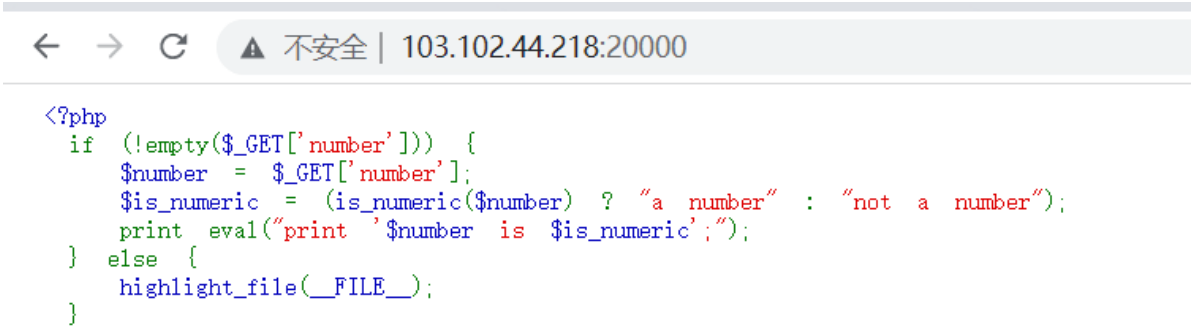


Final flag:




```
flag{now_you_have_the_flag!}
```

task2



```
C:\Users\联想\Desktop>ssh ctf@103.102.44.218 -p 30000
ctf@103.102.44.218's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-89-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Tue Dec  7 00:52:53 2021 from 116.6.234.184
$
```