

picoCTF - RE - Shop writeup

原创

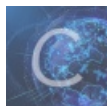
[yyayo](#) 于 2021-07-10 19:10:45 发布 56 收藏

分类专栏: [CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/yyayo/article/details/118639264>

版权



[CTF](#) 专栏收录该内容

10 篇文章 0 订阅

订阅专栏

这个源文件 decompile 之后过于复杂, 之后再研究。直接 nc 然后在上边玩一玩。

```
from pwn import *

p = remote("mercury.picoctf.net", 24851)

p.recv()
p.sendline("0")
p.recv()
p.sendline("-6") # The program doesn't ensure the input is not negative. Or it should use unsigned int variables
.

p.recv()
p.sendline("2")
p.recv()
p.sendline("1")

p.recvuntil("[")

flags_i = p.recvuntil("]", drop=True).decode("utf-8")
flags_i = flags_i.split(" ")

flags = ""

for flag in flags_i:
    flags += chr(int(flag))

print(flags)
```