[Pwn之路]根据所给库，获得远程同环境——使用patchelf的正确姿势

原文：https://www.freebuf.com/sectool/366854.html
存自己这里方便看。

0x00 前言

如何修改本地pwn文件和题目所给环境一致，从而进行调试，这是从学习堆开始就遇到的心头之患。从那以后，直到今天参加完mini LCTF，为了复现一道题目才把这个问题解决掉。网上的博客，参差不齐，由于本人不才，导致都不起作用。故在某学长在校内论坛之中找到正确方法，从而解决了这一心头之患。

并且这里面有一些小问题，也希望请教一下大家。问题我会用Q来表示，欢迎捕捉！

0x01 安装所需软件

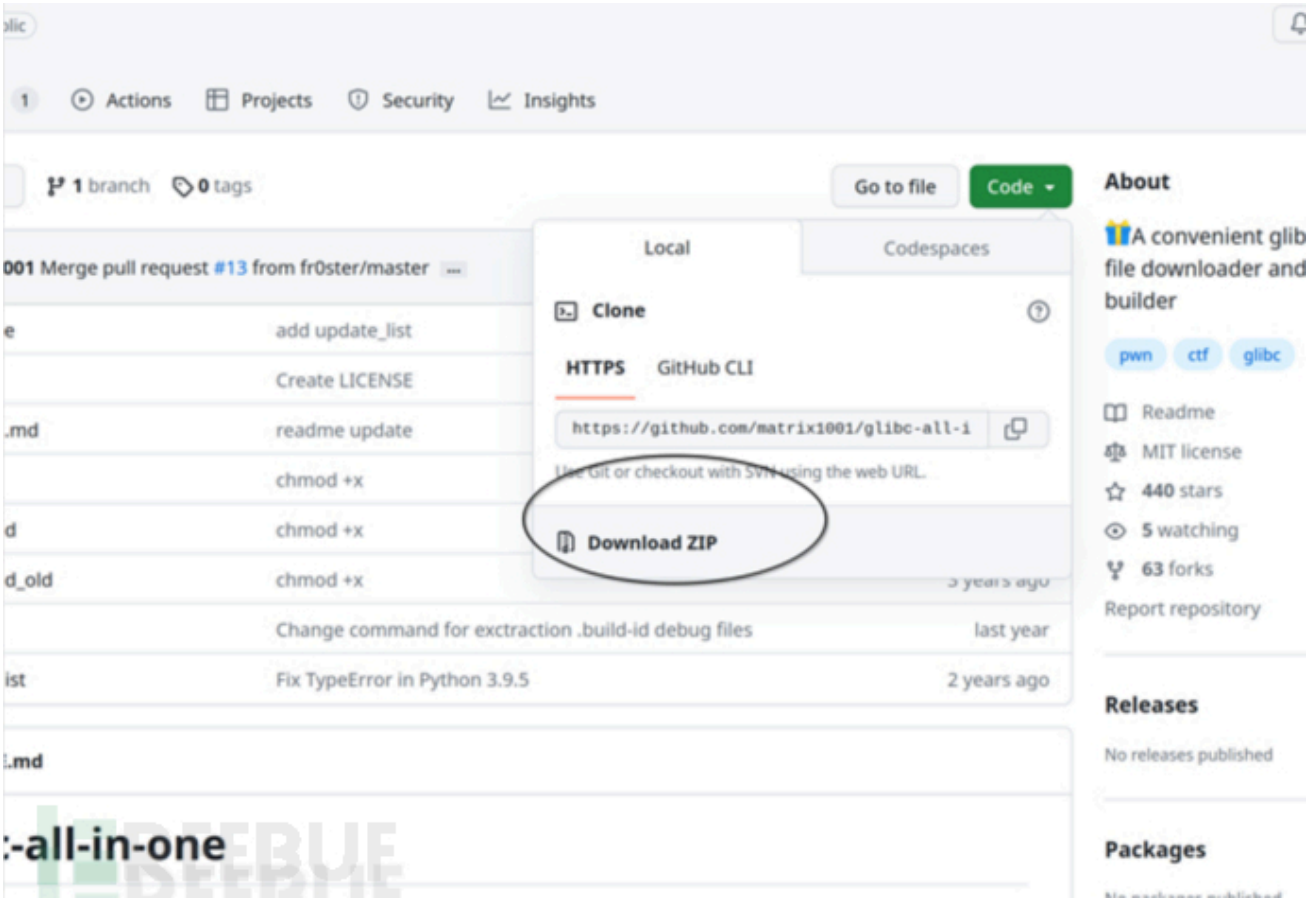
glibc-all-in-one

最快的方式是：

```
git clone https://github.com/matrix1001/glibc-all-in-one.git
cd glibc-all-in-one
chmod a+x build download extract
```

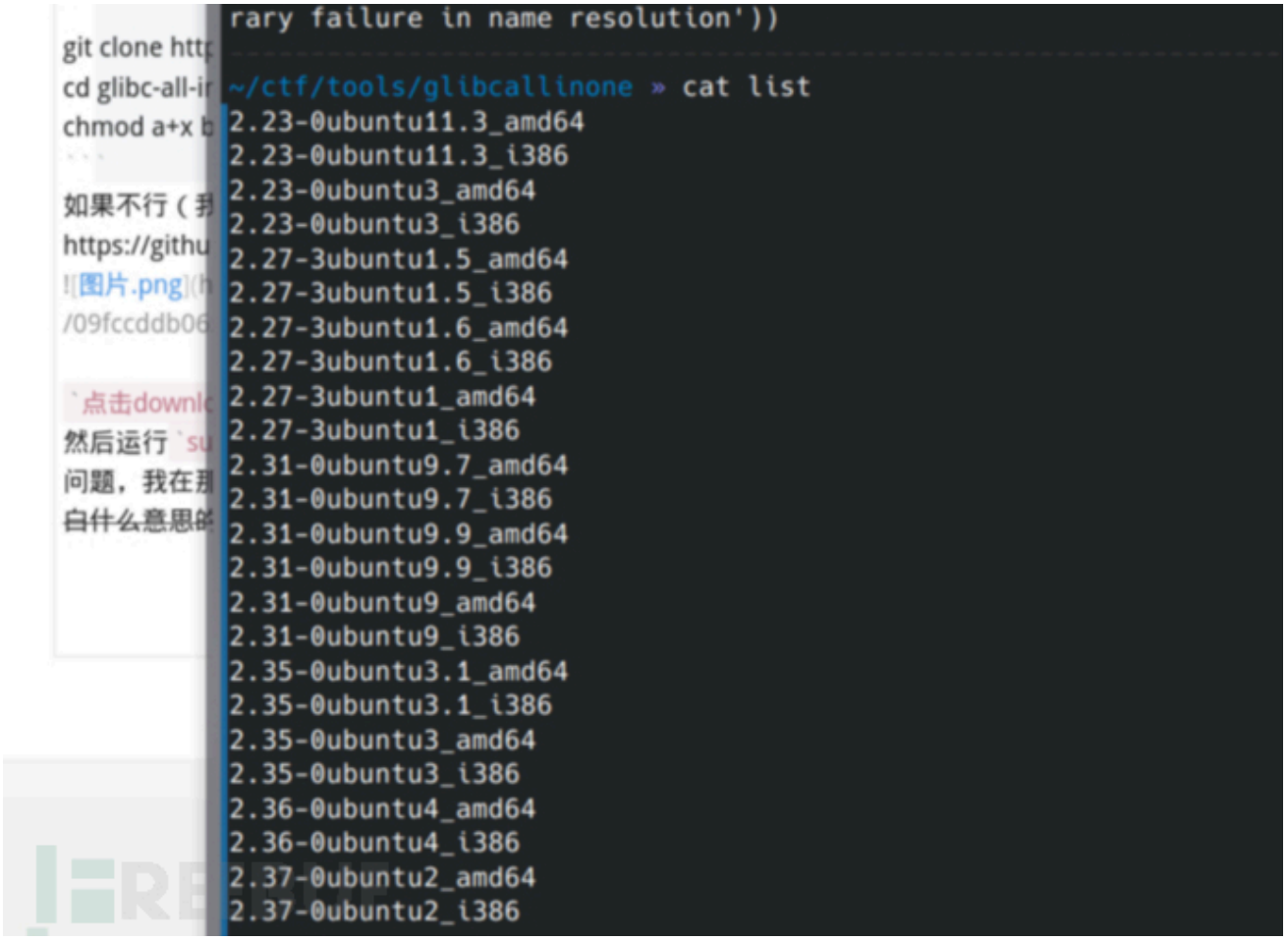
如果不行（我就是不行...），进入下方链接。

> ps：后来发现是ipv6掉认证了



点击download下载，手动解压

然后运行 `sudo python update_list` （如果遇到报错请检查网络问题，我在那里卡了比较久，注意要用direct连接。~~这里不明白什么意思的话不用管我~~），接着 `cat list` 得到包名。



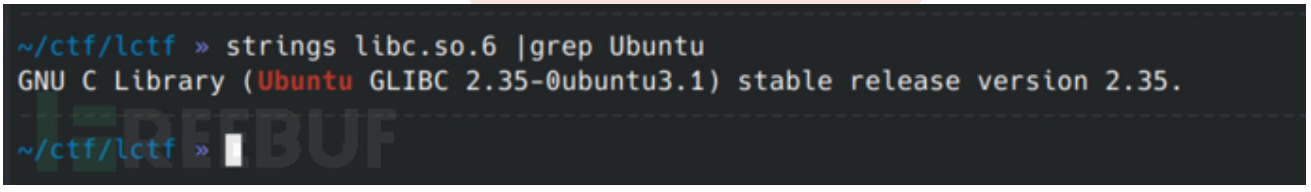
patchelf

我是archlinux，yay patchelf就可以安装好，所以在这里没有遇到什么问题。其他子系统，可以自行搜索，网上的教程很详细，大家可以自行解决。

0x02 确定patch什么库

修改：新增快方法

在有题目所给libc.so.6的目录下直接输入 `strings libc.so.6 |grep Ubuntu` 即可。



1.确定偏移用于搜索

使用ROPgadget

这里的思路我的比较简单，ROPgadget用来查str_bin_sh的地址。

```
ROPgadget --binary libc.so.6 --string '/bin/sh'
```

得到

```
~/ctf/lctf » ROPgadget --binary libc.so.6 --string '/bin/sh'
Strings information
============================================================
0x00000000001d8698 : /bin/sh
```

Q1：那么有没有办法用ROP来查 `printf` ，`system` 之类的地址呢？我暂时没查到相关命令，如果有的话会很简单，不需要接下来的步骤。

使用pwntools

```python
from pwn import *

p = process('./pwn')
libc = ELF('./libc.so.6')
elf = ELF('./pwn')

system = libc.sym['system']#这里的system可以替换成别的函数，用于搜索偏移
print(hex(system))
if args.G:
    gdb.attach(p)

p.interactive()
```

运行。

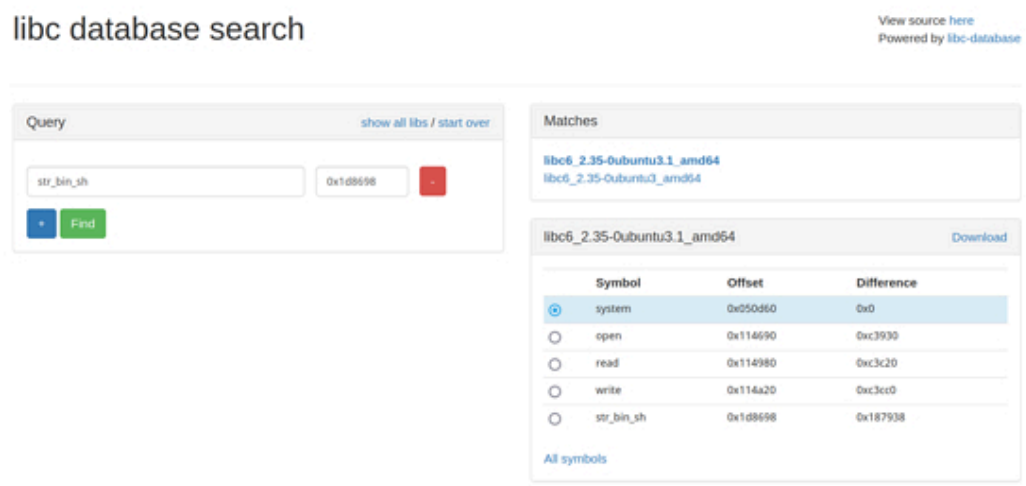
```
~/ctf/lctf » python exp2.py
[+] Starting local process './pwn': pid 40122
[*] '/home/N1nE/ctf/lctf/libc.so.6'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      PIE enabled
[*] '/home/N1nE/ctf/lctf/pwn'
    Arch:     amd64-64-little
    RELRO:    Full RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      PIE enabled
/home/N1nE/ctf/lctf/exp2.py:8: BytesWarning: Text is not bytes; assuming ASCII,
s
  printfadd = p.recvuntil('\n')[-15:-1]
0x50d60
```

`于是我们得知，system的偏移是0x50d60`

3.搜索库

推荐两个网站一起用，找不到的话换另一个，一定要多搜索几个偏移确保没错。其实也可以使用libc-database，不过这个不是这篇文章的重点。

> https://libc.rip/
>
> https://libc.blukat.me/



得到库名。

0x03 下载库

运行 `cat list` 找到2.35-0ubuntu3.1_amd64。

```
~/ctf/tools/glibcallinone » cat list
2.23-0ubuntu11.3_amd64
2.23-0ubuntu11.3_i386
2.23-0ubuntu3_amd64
2.23-0ubuntu3_i386
2.27-3ubuntu1.5_amd64
2.27-3ubuntu1.5_i386
2.27-3ubuntu1.6_amd64
2.27-3ubuntu1.6_i386
2.27-3ubuntu1_amd64
2.27-3ubuntu1_i386
2.31-0ubuntu9.7_amd64
2.31-0ubuntu9.7_i386
2.31-0ubuntu9.9_amd64
2.31-0ubuntu9.9_i386
2.31-0ubuntu9_amd64
2.31-0ubuntu9_i386
2.35-0ubuntu3.1_amd64
2.35-0ubuntu3.1_i386
2.35-0ubuntu3_amd64
2.35-0ubuntu3_i386
2.36-0ubuntu4_amd64
2.36-0ubuntu4_i386
2.37-0ubuntu2_amd64
2.37-0ubuntu2_i386
~/ctf/tools/glibcallinone »
```

cd到年装的glibcallinone的文件夹下。

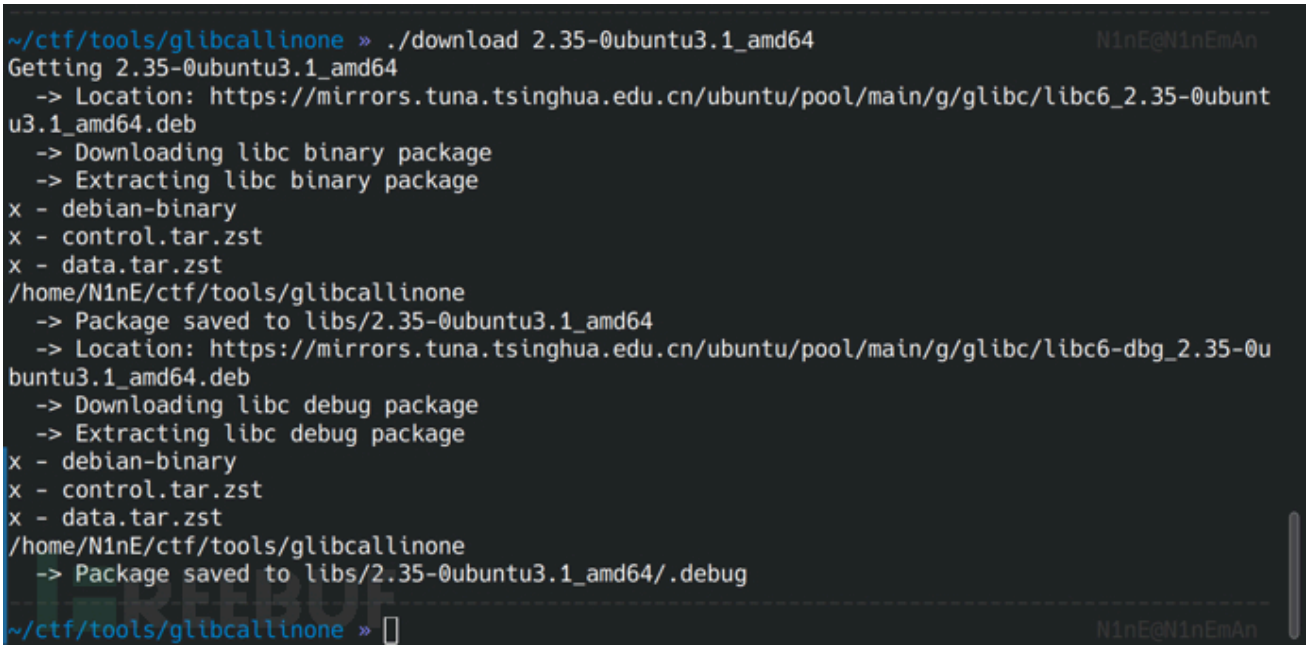
输入 `./download 2.35-0ubuntu3.1_amd64` 即可。
但是我一开始不太一样，我遇到了问题如下：

> ~/ctf/tools/glibcallinone » ./download 2.35-0ubuntu3.1_amd64

> Getting 2.35-0ubuntu3.1_amd64 -> Location:
> https://mirror.tuna.tsinghua.edu.cn/ubuntu/pool/main/g/glibc/libc6_2.35-0ubuntu3.1_amd64.deb
> -> Downloading libc binary package Failed to download package from
> https://mirror.tuna.tsinghua.edu.cn/ubuntu/pool/main/g/glibc/libc6_2.35-0ubuntu3.1_amd64.deb

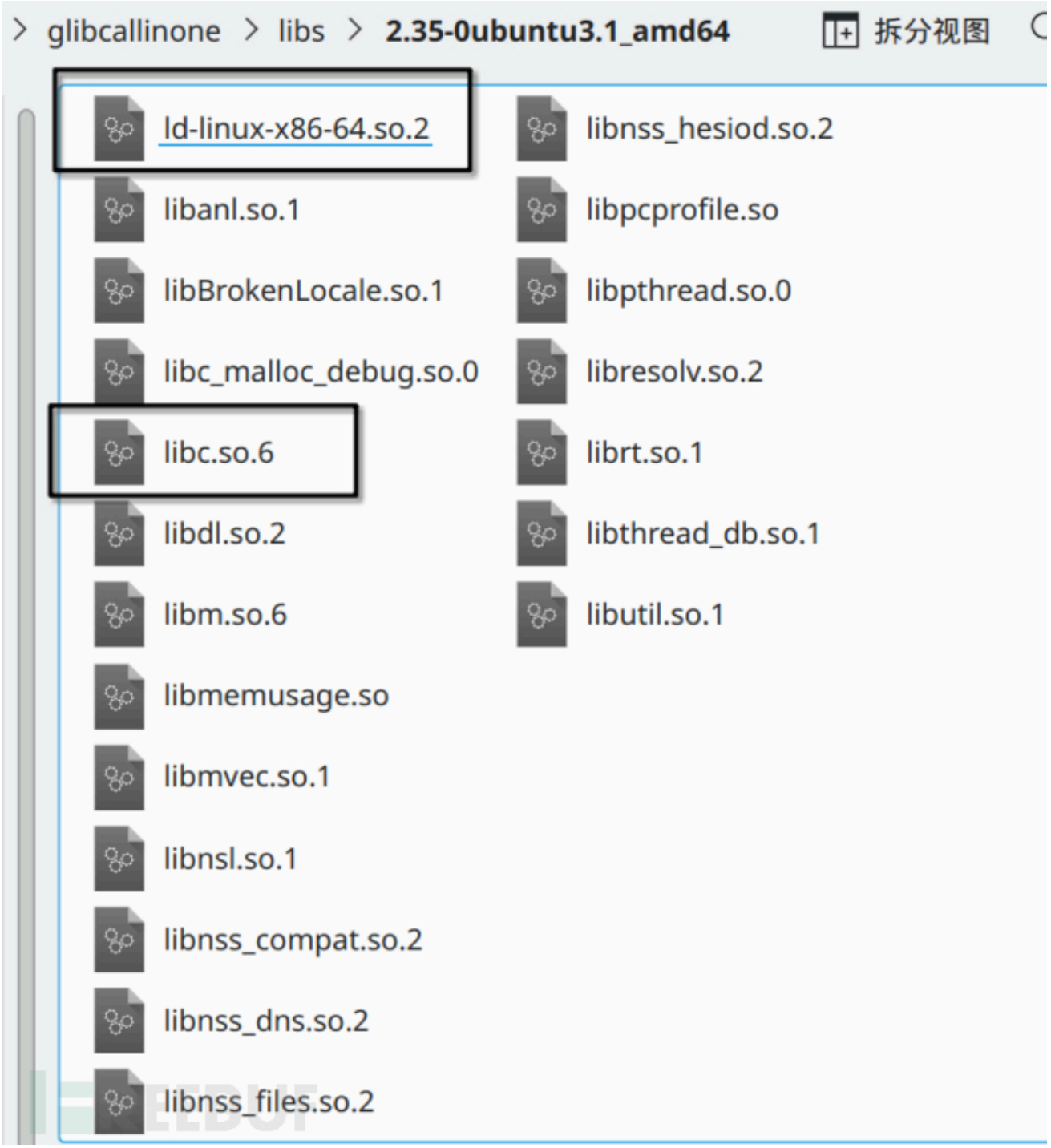
于是只能自己登入，然后解压。

后来发现是没安装wget且校园网ipv6掉认证，重新登陆一下后成功。



0x04 patch!!

找到你的ld和libc.so.6文件。



找到他们的目录，然后在pwn题目文件目录下运行以下两条命令:

```
patchelf --set-interpreter 你的文件目录/ld-linux-x86-64.so.2 ./pwn

patchelf --add-needed 你的文件目录/libc.so.6 ./pwn

patchelf --add-needed 你的目录/libpthread.so.0 ./pwn （如果提示没有libpthread.so.0的话）

#后来发现最好的命令、
patchelf --set-rpath 你的文件目录/ld-linux-x86-64.so.2 ./pwn
```

大功告成。

尾声

动态调试是pwn中必不可少的重要步骤，而patch则是让我们能够动态调试的必由之路。欢迎有任何问题在评论区提出，我们将继续努力走向更高处。

当你没有符号表?

https://www.cnblogs.com/9man/p/17741818.html

posted @ 2023-10-26 22:59 .N1nEmAn 阅读(500) 评论(0)