【PWN系列】XCTF-4-ReeHY-main-100 Writeup

原创

Vicl1fe 于 2020-11-18 15:24:35 发布

分类专栏： pwn

本文链接：https://blog.csdn.net/qq_41918771/article/details/109514415

个人博客地址

```
http://www.darkerbox.com
```

欢迎大家学习交流

参考网址：

```
https://www.cnblogs.com/xingzherufeng/p/9885860.html#commentform
https://blog.csdn.net/seaaseesa/article/details/102907138
```

分析

其实此题有两种解法，一个是整型溢出，一个是double free。因为暂时只搞懂了double free，先写double free的解法

```
[*] '/pwn/xctf/high/4-ReeHY-main-100/4-ReeHY-main'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
```

运行程序大概可以看到有五个功能，增删改查然后加一个退出。

```
root@vicl1fe:/pwn/xctf/high/4-ReeHY-main-100# ./4-ReeHY-main
Input your name:
$ Vic1lfe
Hello Vic1lfe

******************************
Welcome to my black weapon storage!
Now you can use it to do some evil things
1. create exploit
2. delete exploit
3. edit exploit
4. show exploit
5. exit
******************************
$
```


其实查询的功能还在完善。

```
1 int sub_400C42()
2 {
3   return puts("No~No~No~");
4 }
```

看看创建功能。