

# i春秋 - Exploit-Exercises: Nebula - level00

原创

ichalex 于 2017-02-25 13:17:48 发布 2154 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/57079338](https://blog.csdn.net/SCNU_Jiechao/article/details/57079338)

版权



[exploit](#) 专栏收录该内容

13 篇文章 0 订阅

订阅专栏

## About

This level requires you to find a Set User ID program that will run as the "flag00" account. You could also find this by carefully looking in top level directories in / for suspicious looking directories.

Alternatively, look at the find man page.

[Nebula 官网描述](#)

## 思路

如题, 用find找suid的程序

```
find / -user flag00 -perm -4000 2>/dev/null
```

找到1个, 运行之

```
/bin/.../flag00
```

已切换为flag00用户, 获取flag

```
cat /home/flag00/flag
```

```
flag00@nebula:~$ cat /home/flag00/flag  
flag{43H0UTZF0}flag00@nebula:~$
```