# i春秋 - Exploit-Exercises: Nebula - level00

原创

jchalex 于 2017-02-25 13:17:48 发布 2154 收藏

分类专栏： exploit 文章标签： exploit





## 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
```