

Buuctf[ACTF2020 新生赛]Exec

原创

*小瑶 于 2021-06-05 20:13:29 发布 68 收藏

分类专栏: [web](#)

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_52718293/article/details/117603120

版权



[web](#) 专栏收录该内容

32 篇文章 0 订阅

订阅专栏



PING

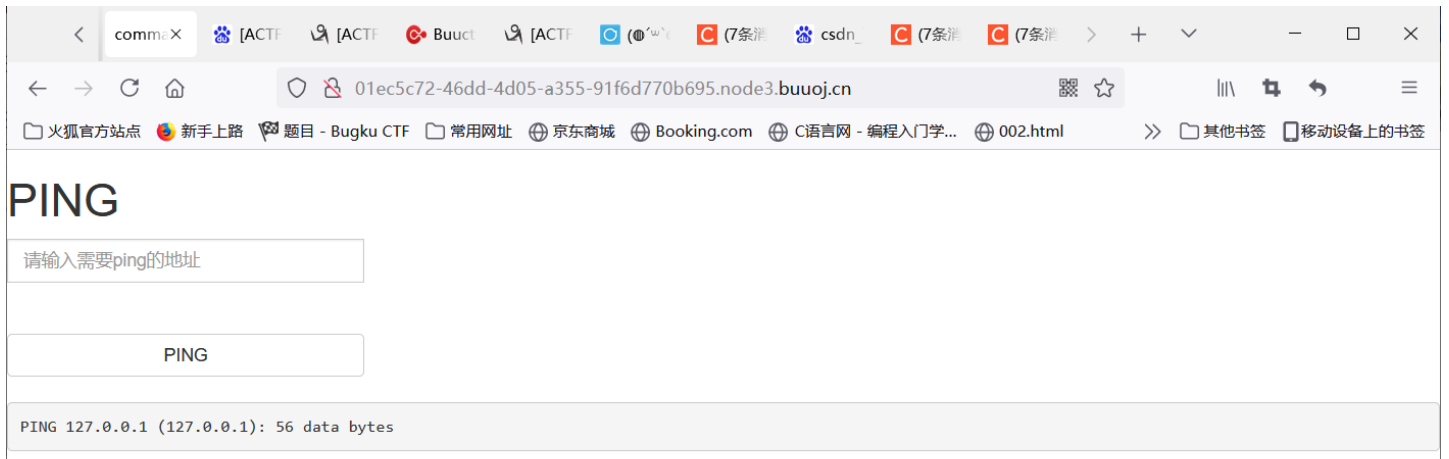
请输入需要ping的地址

PING

https://blog.csdn.net/qq_52718293

打开看到的就是这样的页面, ping命令是用于检查网络联通状况的计算机命令。

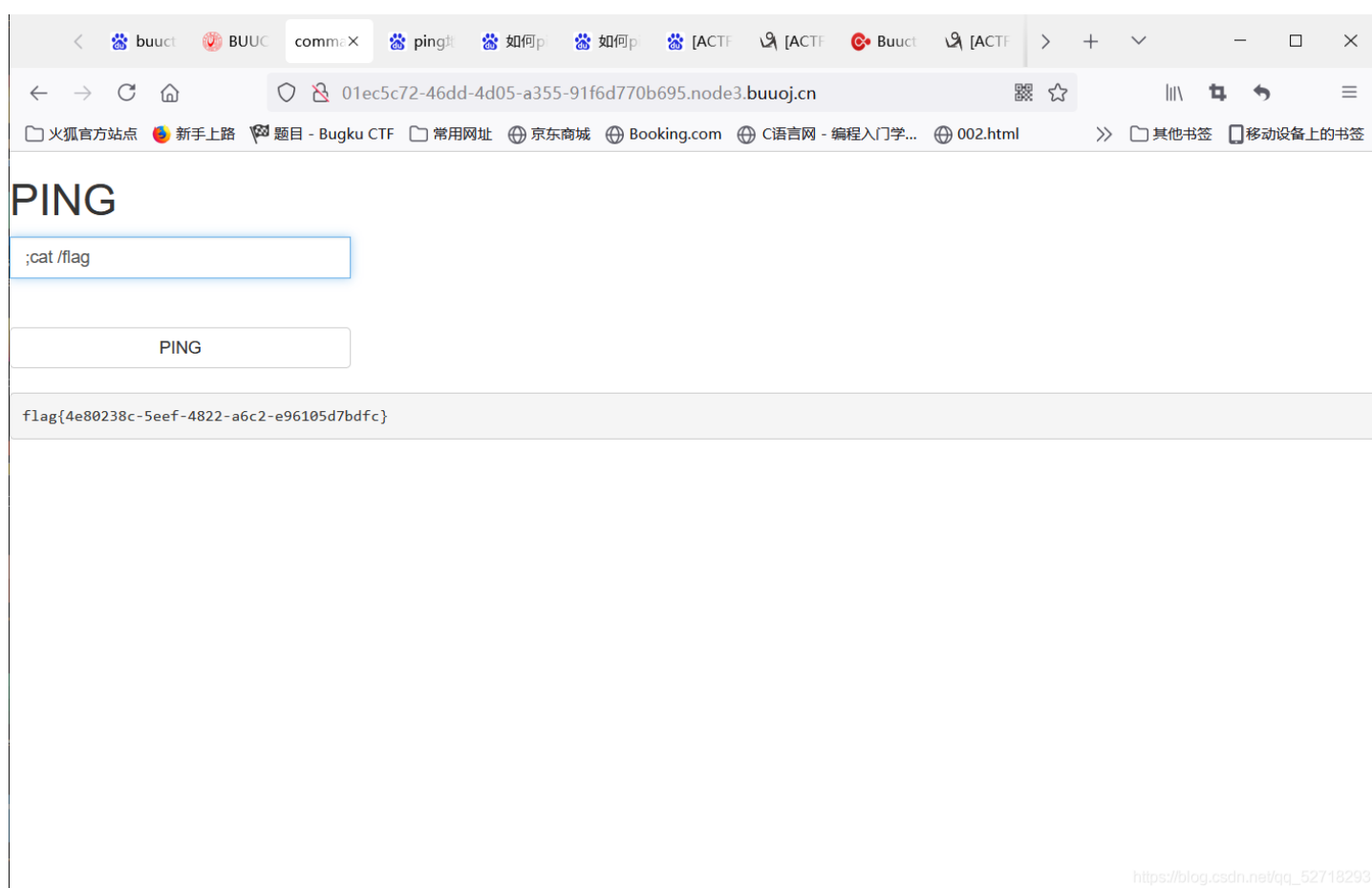
我们可以先尝试着输入一个网址127.0.0.1 然后就得到了这个界面



发现它确实执行了ping的命令，推测可能存在命令执行漏洞

（命令执行漏洞是指服务器没有对执行的命令进行过滤，用户可以随意执行系统命令，命令执行漏洞属于高危漏洞之一）

我们可以试着cat /flag试试



然后就得到了flag

这题考点其实是考常见管道符

（看一下别人总结的）

|（按位或），直接执行|后面的语句

||（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

&（按位与），&前面和后面命令都要执行，无论前面真假

&&（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

;&前后都执行，无论前面真假，同&，（linux也有）