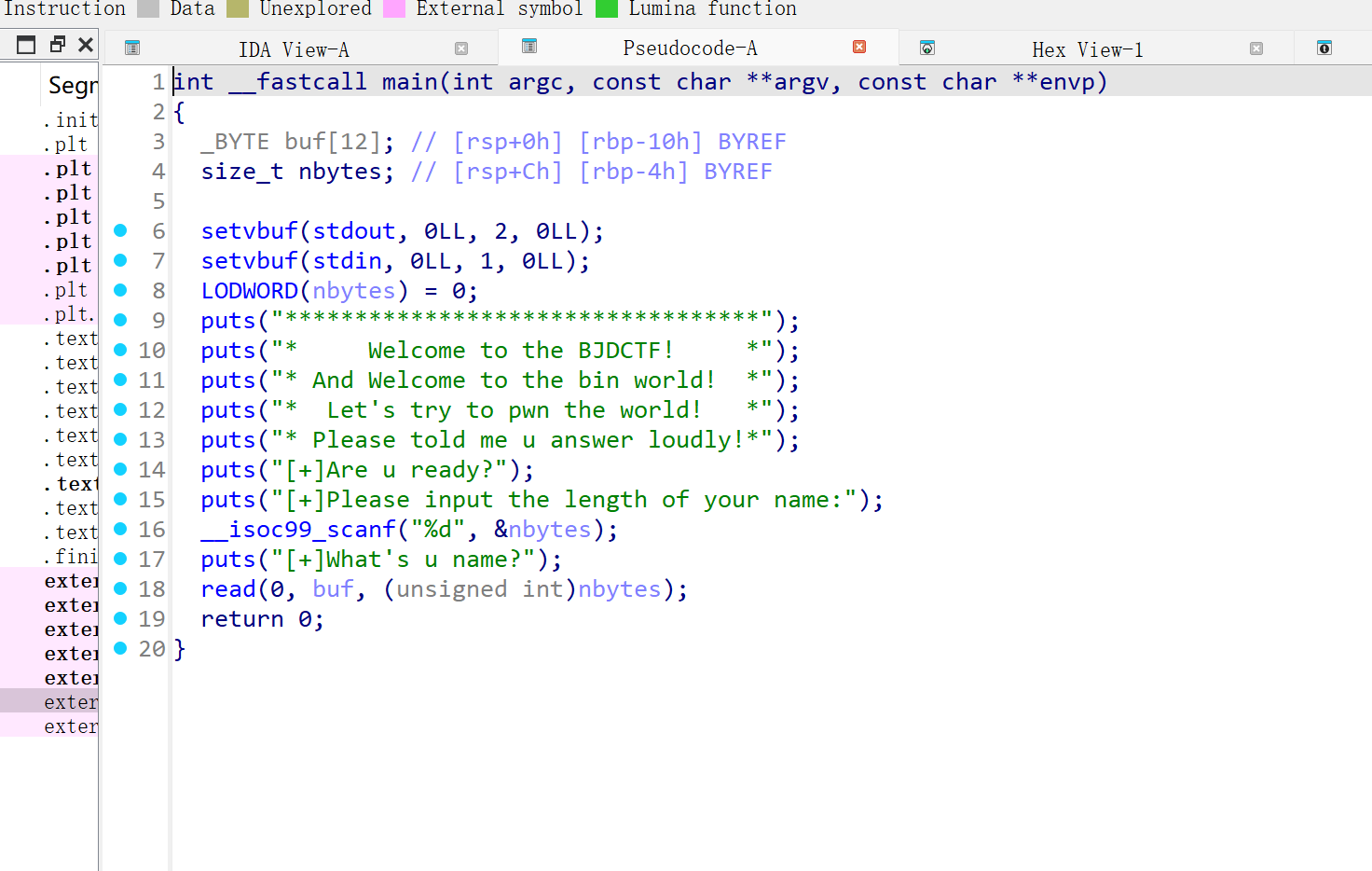
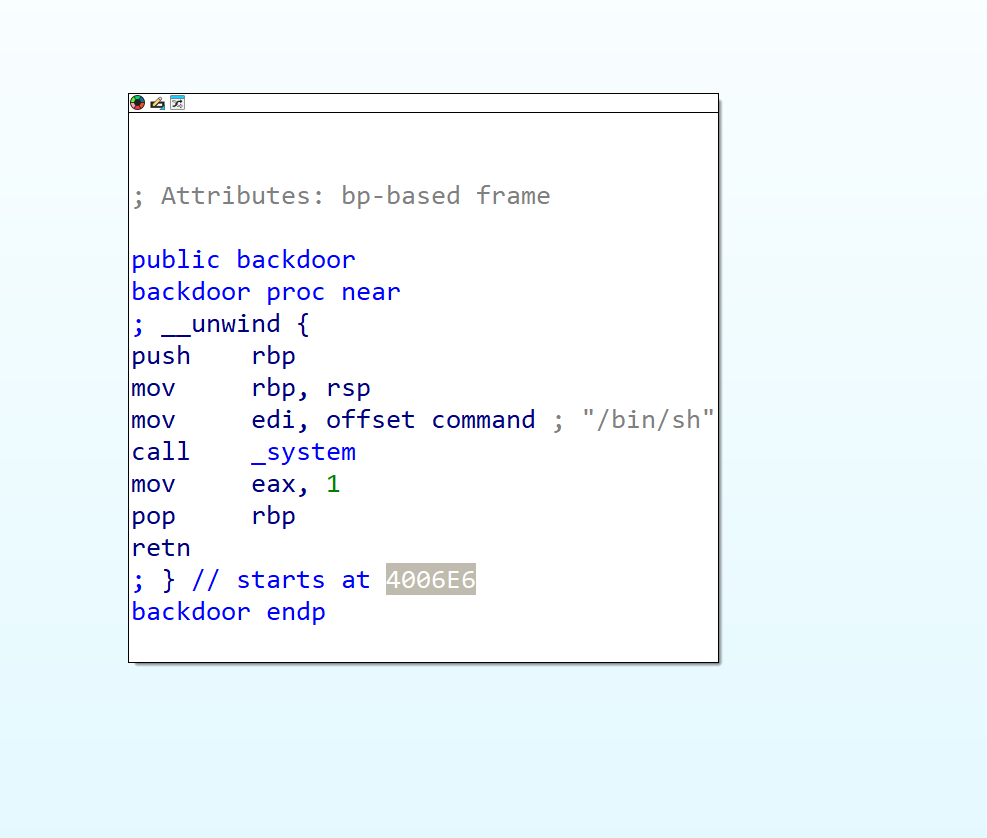
[[BJDCTF 2020]babystack | NSSCTF](https://www.nssctf.cn/problem/705)



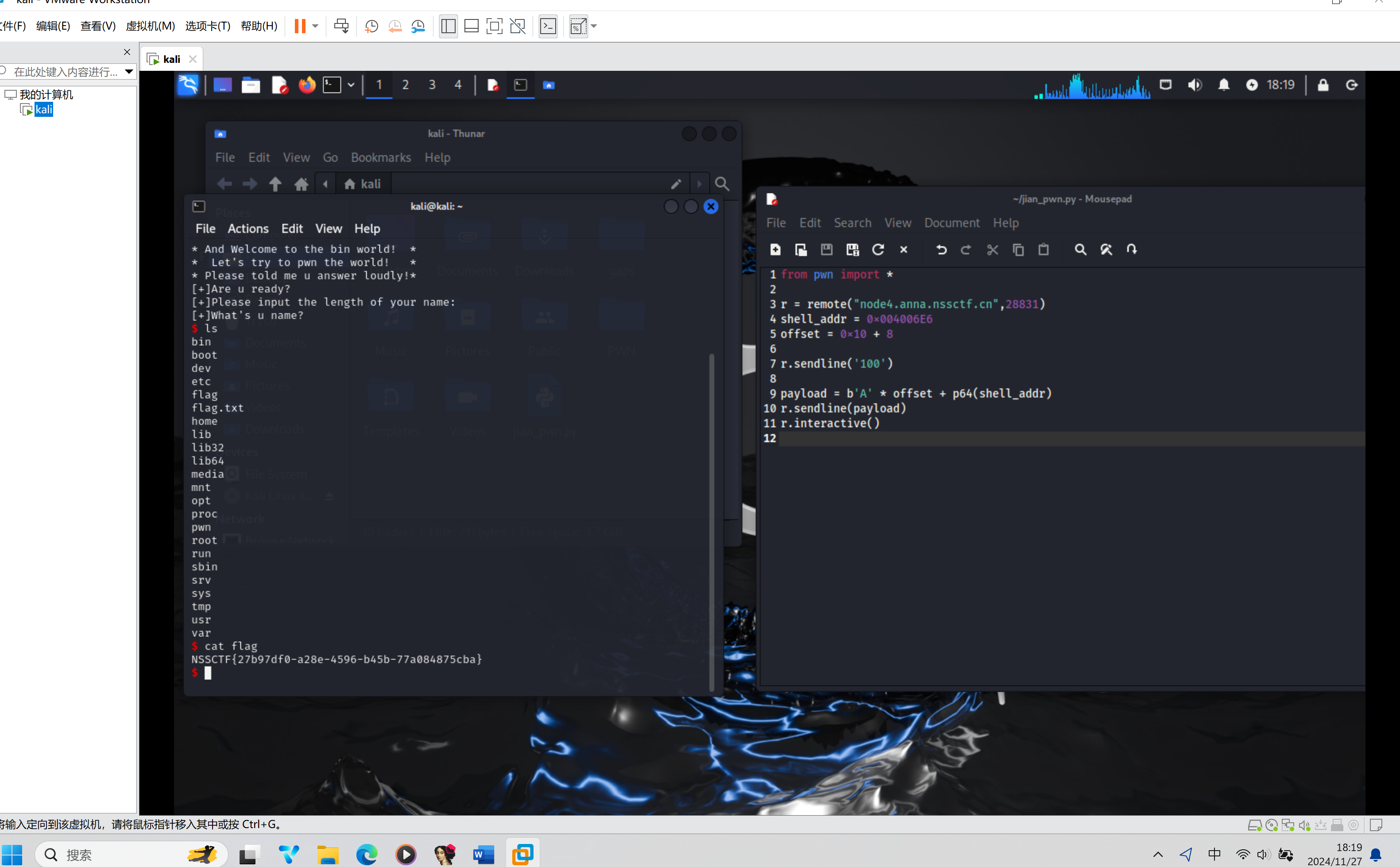
buf读入的数据长度由我们输入的nbytes来控制，所以这里可以利用它来溢出

溢出，查看发现backdoor



那4006E6就是目标地址

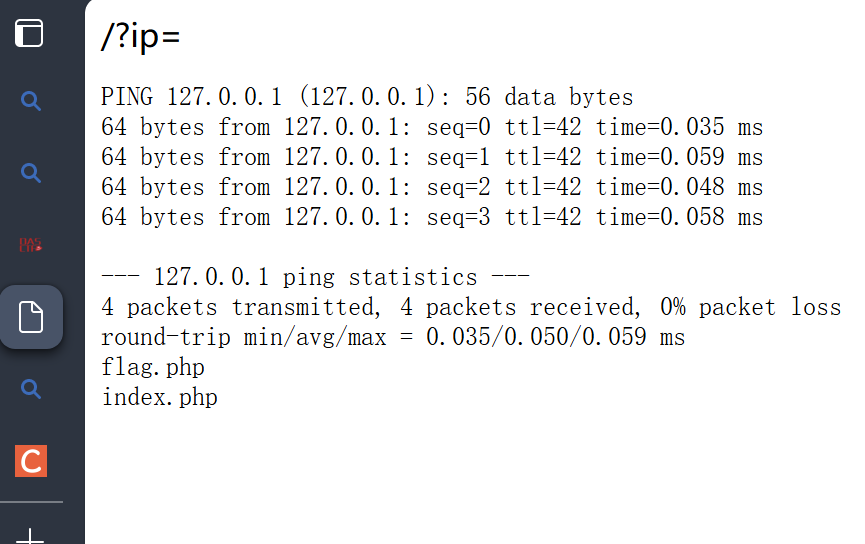
写脚本然后python3



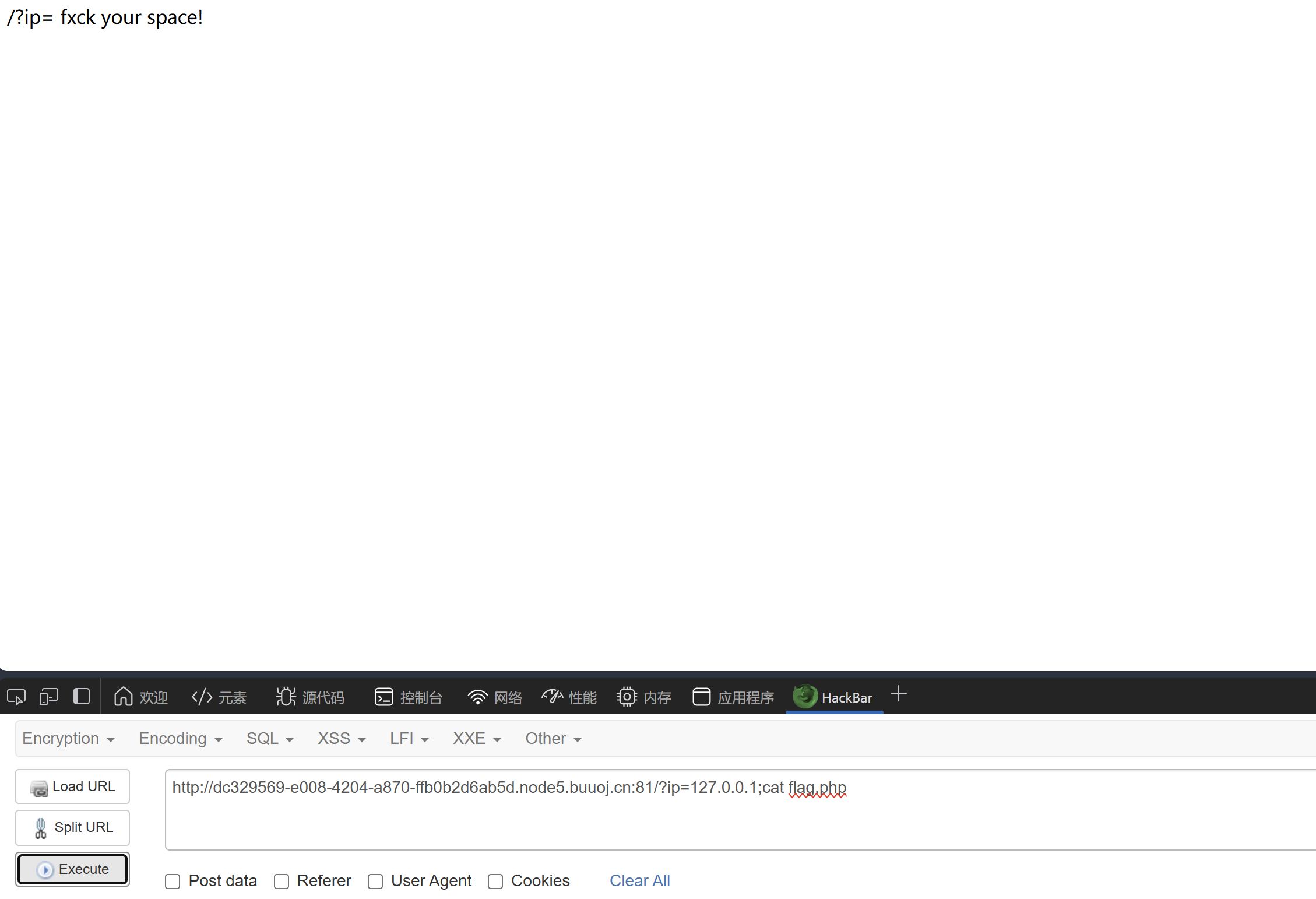
[BUUCTF在线评测](https://buuoj.cn/challenges#[GXYCTF2019]Ping%20Ping%20Ping)

用|或；执行命令





然后。。。。。。



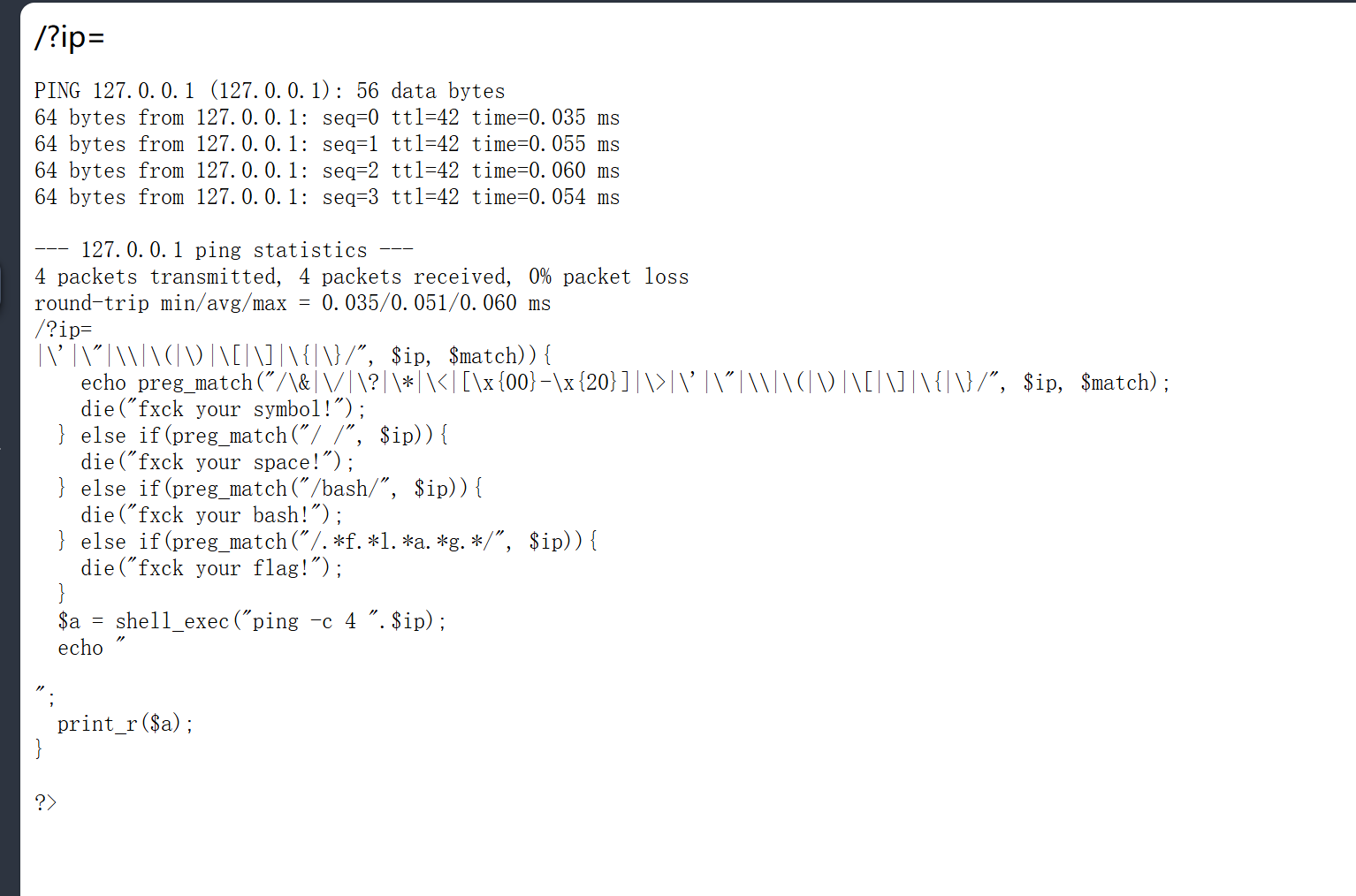
过滤了空格，用${IFS}$代替



Hhhhhh

查看index

源码中有一个$a变量可以覆盖



**简单变量替换，用$a覆盖拼接flag**

?ip=127.0.0.1;a=g;cat$IFS$1fla$a.php

结束

