command execution

解题思路：

- 题目说小宁只写了 ping 没开 waf（web application firewall），那就可以通过在 ping 命令后面夹带东西来获取 shell 的写入权限，我们可以直接把输入框当作 shell 输入界面（只不过它提前帮你输入了 `ping` 四个字母）。

- 首先构造一个句子： `127.0.0.1 && ls` ，填进输入框发过去之后，服务器会执行 ping 命令 **和 ls 命令** ，可以用它来查看当前目录下面都有哪些文件。

- 查看第一层目录，发现只有 index.php，然后就不会了，查阅网上的资料发现全都直奔三级目录，到底为什么他们能直接确定在三级目录里啊！

    仔细想了想，很有可能是把所有的文件夹都试了一遍：先 `127.0.0.1 && ls ../` 进第一层，挨个文件夹找，没有就 `127.0.0.1 && ls ../../` 进第二层，以此类推，直到在第三层的 home 文件夹里找到了 flag。

    提醒了我，可以直接用 `ls ../` 显示当前目录的所有东西，挨个找就完事儿了。

    但这样也未免太傻了。

- 以此为基础，我都进来了，为什么不 **直接用 Linux 里自带的查找命令** 呢？

    于是直接用 `127.0.0.1 && find / -name flag.txt` ，成功，系统返回告诉我： `/home/flag.txt` ，剩下的就不用多说了。

- 最后直接输入： `127.0.0.1 && cat /home/flag.txt` ，服务器直接就把 flag 的内容返回给我们了。