Week 2

What the cow say?

打开题目看见一个输入框，很像以前做到的一个命令执行的题目

试着输入了一下 ls ，发现并没有返回命令执行结果

想到之前看到过的模糊匹配，于是试了一下 ls /*

(后来发现输入 /* 效果是一样的)

可以得到一大堆目录，注意到其中有 /flag_is_here

进一步利用模糊匹配看看这个目录下面有什么

输入 /*e/*得到 /flag_is_here/flag_c0w54y

于是用 cat /*e/*y 来看flag，结果发现cat被禁用了

于是用 'c'at /*e/*y 但是并没有显示命令执行结果，只是返回了输入的东西

问了一下出题的学长，学长说主要问题是连接符|和&被禁用了，要绕过

因为它要先把后面的指令执行后传递给前面的cowsay去执行

搜索了一下，发现反引号可以让其中的命令优先执行

exp：

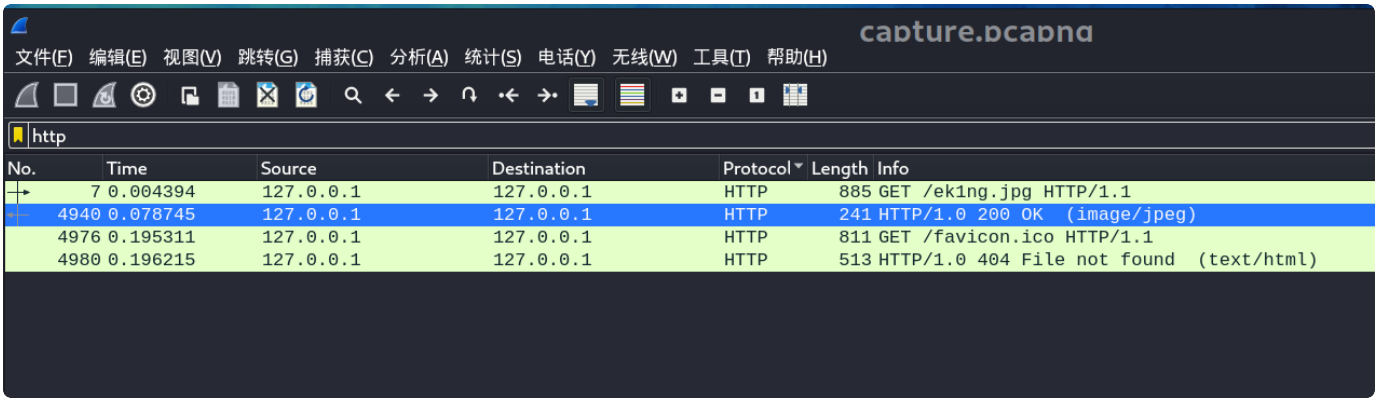
```
`'c'at /*e/*y`
```

midRSA

```
Plain Text
1  from Crypto.Util.number import long_to_bytes
2  m0=13292147408567087351580732082961640130543313742210409432471625281702327748963274496942276607
3  m=m0<<208
4  print(long_to_bytes(m))
```

ek1ng_want_girlfriend

根据提示，到wireshark里面找http流量



第二个是一个图片，导出来看一看

backpack

看附件，应该是要找到一个p，然后enc^p就是flag

```
Plain Text
```

```
from Crypto.Util.number import long_to_bytes
enc=87111417256785349029747857011344936698879376017284464400756682491335008
8148162949968812541218339
flag=enc^0000000000000000000000000000000
print(long_to_bytes(flag))
```

得到：

```
b'hgame{M@ster_0f ba3kpack_m4nag3ment!}\x00\x0e#'
```