

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=132921474085670873515807320829616401305433137422104094324716252817023277
   48963274496942276607
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

capture.pcapng

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

http

No.	Time	Source	Destination	Protocol	Length	Info
7	0.004394	127.0.0.1	127.0.0.1	HTTP	885	GET /eking.jpg HTTP/1.1
4940	0.078745	127.0.0.1	127.0.0.1	HTTP	241	HTTP/1.0 200 OK (image/jpeg)
4976	0.195311	127.0.0.1	127.0.0.1	HTTP	811	GET /favicon.ico HTTP/1.1
4980	0.196215	127.0.0.1	127.0.0.1	HTTP	513	HTTP/1.0 404 File not found (text/html)

第二个是一个图片，导出来看一看



hgame{ek1ng_want_girlfriend_qq_761042182}

backpack

看附件，应该是要找到一个p，然后enc^p就是flag

```
▼ Plain Text |
1  from Crypto.Util.number import long_to_bytes
2  enc=87111417256785349029747857011344936698879376017284464400756682491335008
   8148162949968812541218339
3  flag=enc^0000000000000000000000000000000000
4  print(long_to_bytes(flag))
```

得到：

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