ctfshow 月饼杯(第二届) 部分WriteUp

原创

是Mumuzi 于 2021-09-21 08:00:32 发布 1789 收藏 11

分类专栏： ctf ctfshow 文章标签： 区块链

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

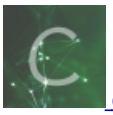
本文链接：https://blog.csdn.net/qq_42880719/article/details/120387812

版权

ctf 同时被 2 个专栏收录

75 篇文章 28 订阅

订阅专栏



ctfshow

23 篇文章 8 订阅

订阅专栏

Misc

杂项签到

右键附件，从链接另存文件。然后用16进制编辑器或者你想用notepad也彳亍看文件尾，有一串base64，解码即可。

```
ctfshow{we1come_to_mooncake_cap}
```

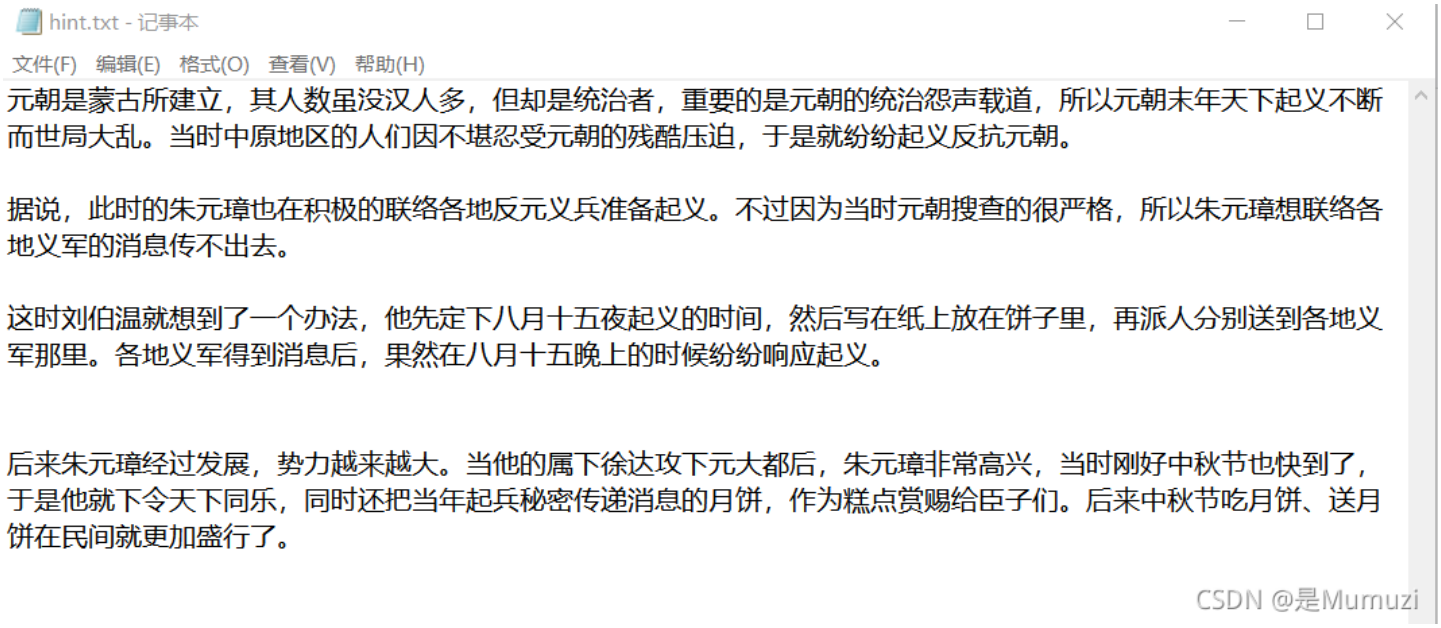
有手就行

查看exif，有一串阿拉伯语，翻译过来是“你知道汉明码吗”
查看图片文件尾，发现一串数字
10110110111
然后随便找一篇看一下是怎么编码的，以及如何纠错的
https://blog.csdn.net/qq_19782019/article/details/87452394
例子他举的也挺详细了，个人看。
首先看1号校验位，提取出来分别是
1 1 0 1 1 1 看起来是采用的奇效验
再看2号校验位管理的
1 0 0 1 1 1，有4个1，偶校验吗？
再看3号
0 1 1 0 偶
4号
1 0 1 1 奇
然后问了一下出题人长度是不是11他说不是
emmmmmm
所以这串是那篇文章里的m,题目其实是少了校验码。。
所以完整的应该是
1011011a011b1cd
首先1号那个校验的区域为
1 1 0 1 0 1 1 d
2号为
1 0 0 1 0 1 1 c
3号为
1 0 1 1 0 1 1 b
4号为
1 0 1 1 0 1 1 a
若为奇效验位则：
a = 0,b = 0,c = 1,d = 0
若为偶效验位则:
a = 1,b = 1,c = 0,d = 1
得到两串
101101100110110
101101110111101
尝试提交发现偶校验的是正确的

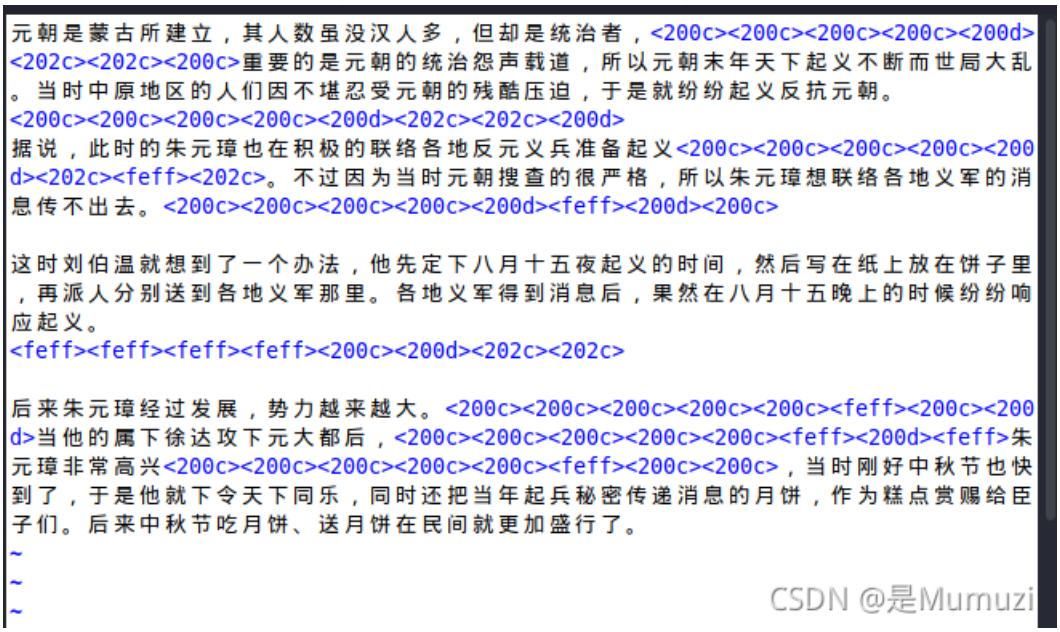
> ctfshow{101101110111101}

月饼起义

600多kb解压只有1kb，那可不行。先看看hint，hint改成hint.txt

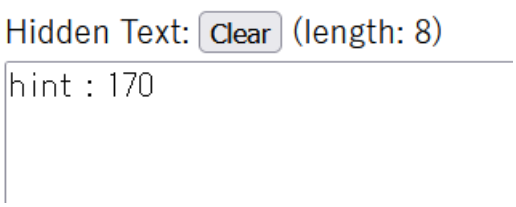


然后发现某些行，藏的有类似零宽的，于是在kali下打开



不愧是我(

勾选U+200C、U+200D、U+202C、U+202D(就是默认的那串)



hint看完了，010打开看一下zip
会发现正常zip后面有一串奇怪的东西，然后再后面就是不知道啥东西
拉到文件尾，还能看到一个PK标识。
170居然是异或。。。
用010打开,全选，然后选择 工具—十六进制运算—二进制异或—无符号字节，170
然后再看文件尾，发现是倒过来的PNG

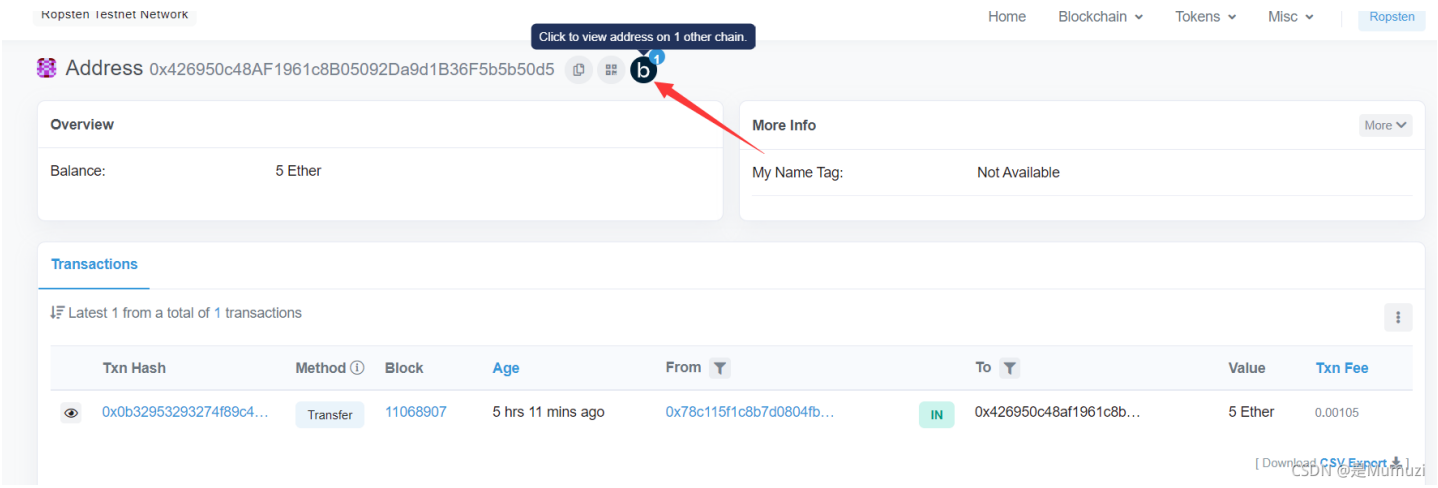
```
f = open('1.zip','rb').read()
f1 = open('2.zip','wb')
f1.write(f[::-1])
```

改成png，再删掉开头多余部分即可，得到一张纯黑的图，发现有LSB隐写
结果又藏了一张png，save bin下来

> ctfshow{I_hate_Wuren_m00n_cakes}

HelloFlag

首先根据合约地址，去访问一下看看
https://ropsten.etherscan.io/address/0x426950c48af1961c8b05092da9d1b36f5b5b50d5
其实谷歌搜索一下，就只能怎么看了
但我的做法是这样的



去看其他链
然后点过去查看地址0x6d1148e6ee8a1c661a81622825f32da633371f278a8af2e5d9a4950b6fda5f8a
然后看一下data，最后有一个7d明显是}，转一下码即可

> ctfshow{pr1vate__1s_N0t_prIv4t3}

感觉应该是故意放的吧。或者非预期

Project Tao-1

没人出2就不放2,图片懒得复制粘贴，不放。

第0关：W4lc0me
下一关为Letsstart

第1关:Letsstart
源代码能看到一个/some_informations

第二关：根据名字可知，some_informations是错误的，毕竟information不可数，所以下一关为some_information

第3关
可爱的色块
颜色的R、G、B值按 ASCII 转为字符串即可得到下一关

> G0od! Next is /CTFG0d

访问/CTFG0d

第4关 被子
当然是base啦
解密为base64—base16—base64—base32—reverse
得到/N4xtplace

第5关
AAencode解码得到
/cftla5gsh0w

第6关
这题应该挺卡人的，主要是可能想不到（但是这题是有人出过的，解的话还不少），首先页面的标题叫no flag here
然后log文件里面也有一个密文，解码方式其实就是

```
s2 = r'nn]ch\aXe\WcgR``OUMYKLIP'
for i in range(len(s2)):
    print(chr(ord(s2[i])+i),end='')
#no_flag_means_no_f_l_a_g
```

意思是把这四个字母去掉，/cftla5gsh0w去掉flag为
/ct5sh0w

第7关
向下拉能看见一个打乱的二维码，手动修复一下即可。3*3
扫码得到/t308g0d

第8关(flag关)
有个附件，下载下来是一个压缩包，伪加密而已啦。
图片的话，改个高度就行

> Flag为：ctfshow{easy_half_and_Ez_flag}

Project Tao-2

下一关的话，根据提示
套:那东西在哪啊？

神:寸头男子是看不到图片上不上写了吗？
[获得碎片提示]
注意大小写
嗯，下一关就是/DEADSOUL

第9关
题目问的是你知道知乎在后台日志埋藏了一个彩蛋吗？(注意大小写)
知乎在控制台放了一个招人的广告

CSDN @是Mumuzi

所以下一关为/HIRE

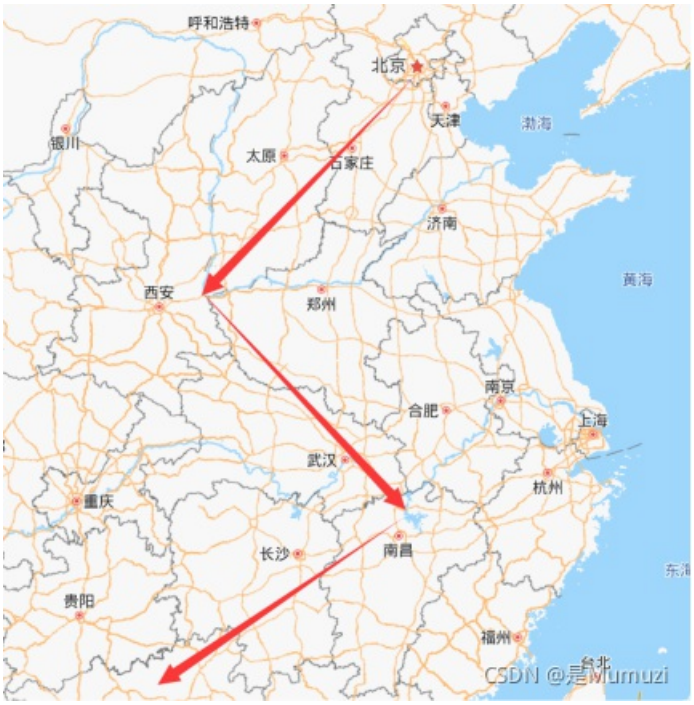
第10关是一张图
Log文件可以获得提示
神:那你就不能访问一下这张图吗？ 12:05:28
[获得碎片提示]
解开后注意最下面，答案请将某两(A开头)单词中间添加下划线
用PIL读取一下这张图

```
from PIL import Image
pic = Image.open('index.png')
print(pic.getpixel((5,5)))
```

得到(14, 215, 177, 38)
将其转为IP格式
14.215.177.38
跳转到了baidu的首页
而最下方有个About Baidu
所以之后访问/About_Baidu

第11关
地名
巴山夜雨涨秋池，长安大道连狭邪。自笑平生无所着，此地空余黄鹤楼。
分别对应
川渝—西安—郑州—武汉

前不见古人，黄河入海流。灵山多秀色，西北是融州。
分别对应
北京—山西拥挤—庐山—柳川



地图上看就是ns
所以访问/ns
当然这里很明显是2个字母，你也可以python用request找到

第12关
老考点
看log文件知道是摩斯，但是访问/SAYL7UNIT又不正确，所以应该是摩斯的.和-反过来了，先加密然后将长短调换一下即可得到正确的
/ONLY2GAME

第13关
-…/…–/--…/.–.-/…–./.–…/…–/-…-.
虽然看起来是梅开二度，但是老玩家一看就知道是博多，并且源代码注释提示了fw bits，其实是five bits，就是5bit编码
博多码，
-换成1，.换成0即可
https://www.boxentriq.com/code-breaking/baudot-code
10000 00011 11000 01101 00110 01100 00011 10010
得到TAOFINAL
根据log文件，需要小写
/taofinal

第14关
下载flag文件，文件尾即flag
很简单吧

```
ctfshow{this_is_a_ez_try_cuz_no_time}
```

问个问题，你猜log还有什么地方可以用？

Web

Web签到

md5之前和之后要相同，正好省赛做过，所以传参

```
?YBB=0e215962017
```

OSINT

以卵击石

首先百度识图（切记用手机），然后直接能看到的就是Mr & Mrs开头的，再往下翻可以看到“柠檬挞”三个字
直接去大众点评搜“Mr & Mrs Bund”，定位为上海，查看第一个就彳亍

CSDN @是Mumuzi

110块钱
然后说是B站是吧，既然要复刻，肯定是放美食区去了
然后搜一下柠檬挞，发现没一个像样的。。。
然后搜柠檬，我看到绵羊料理的标题是，一个柠檬100块，点进去一看，对就是她了，然后看一下视频

除去7号的话，内陷就是6。
提交该视频BV号是错误的，然后题目也说是第一次提到，想必在8月6号之前就提到过，于是查看动态，结果还是在评论区找到某两位高质量男性，分别是雨哥和力元君，看他两视频就发现在第一期蹭饭挑战中找到了绵羊
所以flag为

> ctfshow{110_6_BV1664y1W7zS}

幸福小镇

直接百度名字就可以看到了

> ctfshow{可米_杨鸥}

PS打卡第一天

下载下来改成.psd，用PS打开
然后把冬天的保存下来，百度识图

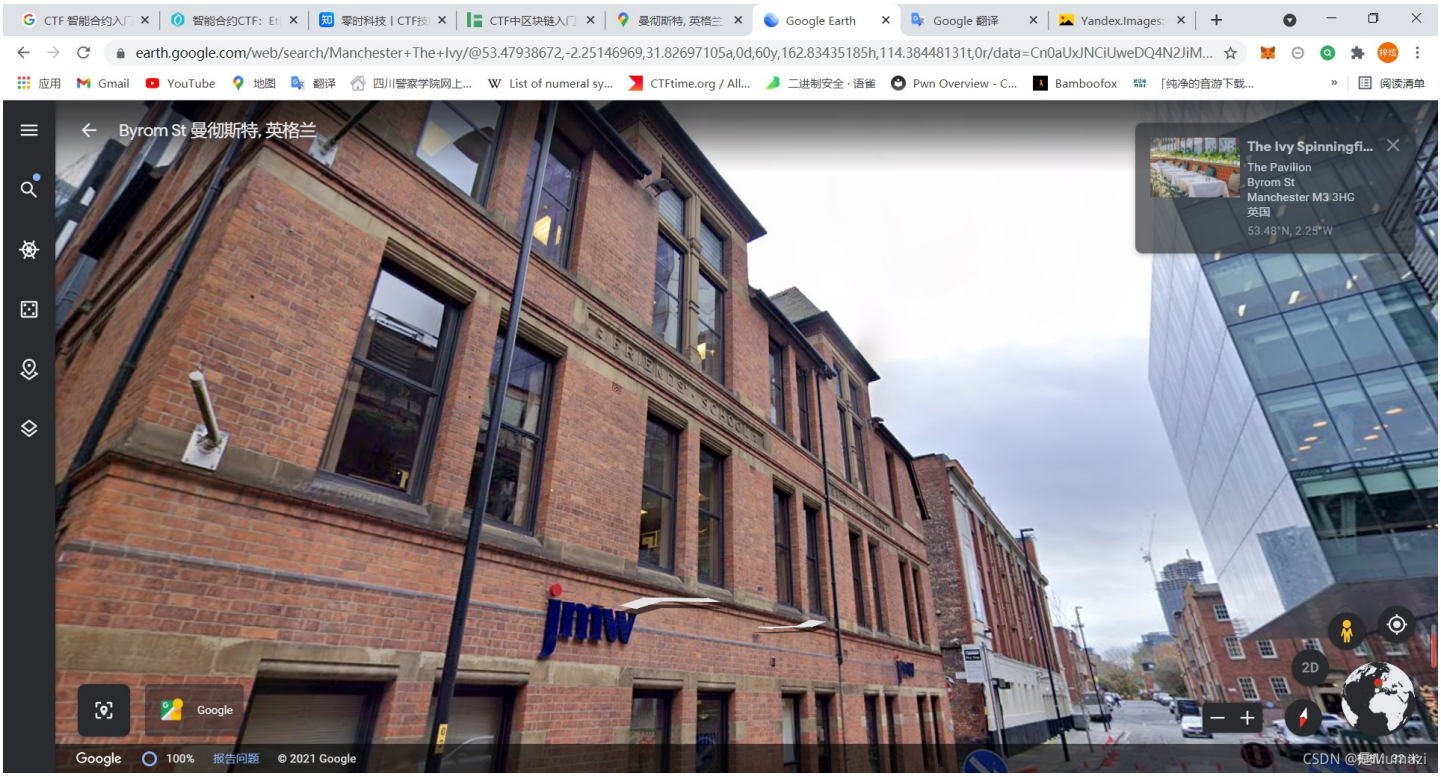
网站已经打不开了，直接搜lzu

然后再去百度兰州大学即可

```
ctfshow{Lanzhou_University}
```

抬头看看

首先百度识图，然后找到文章
发现这里，弗爵在曼联著名的「The Ivy」餐厅
于是谷歌地球搜Manchester The Ivy
搜到了The Ivy Spinningfields Manchester
查看街景
https://earth.google.com/web/search/Manchester+The+Ivy/@53.47938672,-2.25146969,31.82697105a,0d,60y,162.83435185h,114.38448131t,0r/data=Cn0aUxJNCiUweDQ4N2JiMThjNzl2MWMxODE6MHhmMjljODZmMGMzMmRiZmMxGbuK1ptivUpAISPKzSZ2AwLAKhJNYW5jaGVzdGVylFRoZSBJdnkYASABIiYKJAI6R3TVcWT4PxF5jdlmSSr0PxlxGMrMpwFaQCHcU-DGsN1ZQCIaChZHLXNzR1hKSjBYT2VMOHNfcGRUTFVnEAI



> ctfshow{FRIENDSSCHOOL}

见字如面

根据hint2找到的。

然后百度识图得知名字是山姆·阿勒代斯
在这个贴吧里搜阿勒代斯没有找到，但是搜山姆

然后去看一下卖这个的人的QQ

> ctfshow{893332587}

套套去哪儿

映入眼帘的B6467，日期是6月3号，时间是下午，用飞常准看一看TV9817、GJ5039、ZH3721。根据此时的影子可以判断，太阳在飞机斜左侧，所以飞机目前是自南偏西像北偏东飞行。可以排除13:00-15:20的航班和晚上18:45起飞的航班，剩下的都是16:00-17:55的航班。而起点和终点三个航班都相同，只能爆破一下了，下载的目标是找到下方城市。
虽然此时也能慢慢爆破，但是还是麻烦，一个个来看吧。
可以根据飞机来判断时间，首先随便选一个，这里选TV9817吧，搜索之后跳转到飞常准的网页，查到AIRBUSA319-115 ，然后去百度，得到一个信息机高11.76，翼展 ：34.09米。但是机高相对于地面11.76，相对于机翼其实大概是5左右，再看图片，基本正好是一ban，所以此时tan角约等于2.5(有误差)
，计算大概得到为68°，再去看看当天日出日落。因为不知道此时是哪，于是取个平均，6点~19:30,180°来平分，相当于每分钟0.22222°，算一下大概在下午5:50左右。看了一下大概就太原、吕梁、长治、临汾、延安等几个地周围，但是这样判断肯定是不对的！只是捋个大概，然后剩下的就只有河流。此时就只有想办法对比河流。

哦！！！想起来了，此时是自南偏西像北偏东飞行，能直接再排除黄帝陵到乱石沟、某个山脊到美信集团玫瑰种植加工基地这两个部分，还有最后大转弯的部分
有黄有绿，对比地图是西安到太原这段，也是在5点之后，感觉时间上大概是正确的。然后放大沿航线找河流。这中间基本上是没有河流的，所以相对来说比较好找到。
沿路上发现了，湖、湖、……
然后我才发现，把捏码错误的地方排除之后，那些地方几乎都是县，没啥市。。
最后其实真的不想去找了，大概时间锁定在了5:10~5:30这段，而这段经过的市只有延安市，因此就只有延安市+3个航班其中一个

> ctfshow{延安TV9817}

最后发现，瞎用影子推算的时间差了接近半个多小时。毕竟没把夏天这个因素放进去计算。。还好出题人没问的更精细。

Crypto

我的木头啊！！！

> 题目：
> c6_l_@t216MG_0q_Uf673JTYYzBXs{31QJmTTg=hw63XZFZiHho5GzE}

根据描述先栅栏
W型栅栏,6 http://www.metools.info/code/fence154.html

> ctfshow{626173653136_MJQXGZJTGI_YmFzZTY0_qzTiEHgB_@UX=h}

看了一下，应该是分别解码
第一坨数字base16
第二坨大写base32
第三坨直接base64
第四坨尝试base58
第五坨发现base85
组合得到

> ctfshow{base16_base32_base64_base58_base}

一封信

不能直接访问，还是又键然后另存为附件
emoji，然后末尾是两个记事本(好像是
直接emoji-aes，秘钥就是mooncake
https://aghorler.github.io/emoji-aes/

> ctfshow{Happy_Mid-Autumn_Festival}