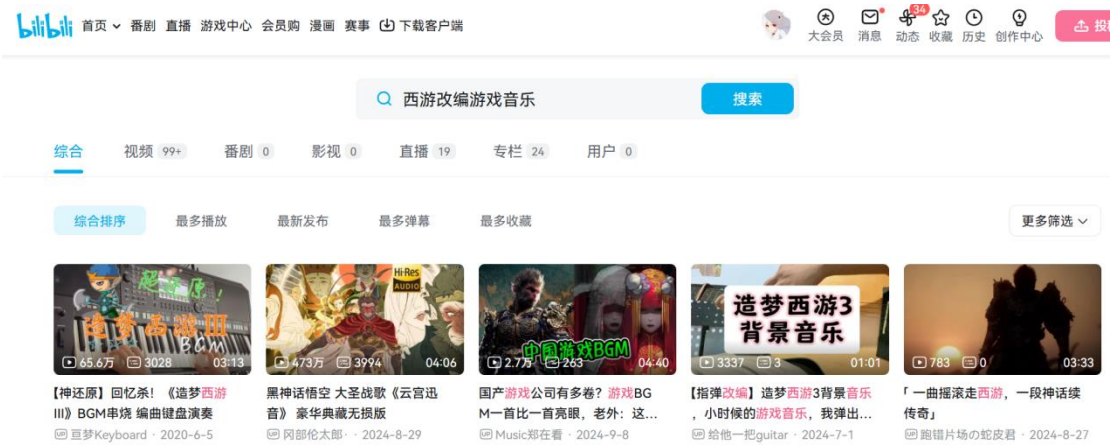
Egg Team Wp

[Misc]

A 签到题

注意到题目里描述了天庭，盲猜西游记，加上有说钢琴改编，b 站搜索



furryCTF{zaomengxiyou3}

B 猫猫的故事

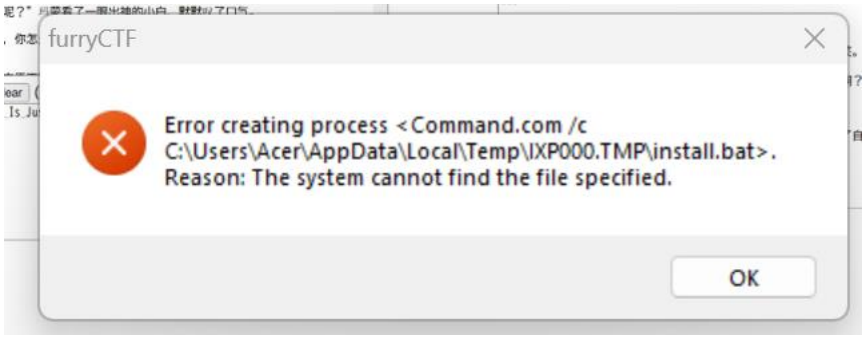
左键 inspect 注意到很多空白字符，应该是某种隐写，搜了一下“zwnj 隐写”，发现是零宽度隐写，使用网站

https://330k.github.io/misc_tools/unicode_steganography.html

解密得

C 安装包

启动附件，得到报错提示



到对应路径下查看有什么文件

找到 f12g.txt

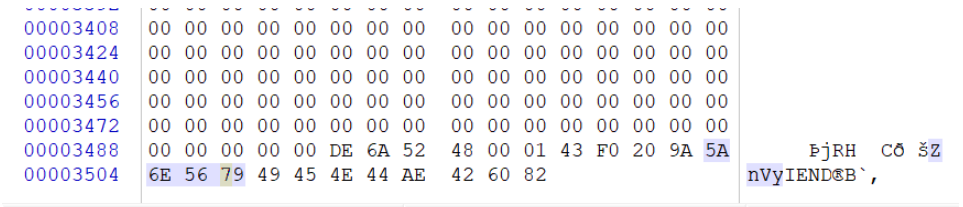
看样子是变换了，rot 几次，得到几个字符串，拼凑出最后 flag

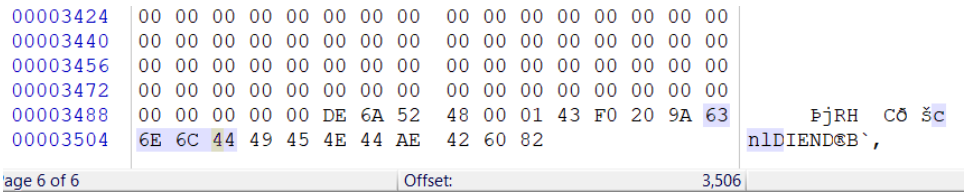
```
koiiwEMK{M0q_Kf_Fkwj_K12a_Ze_Gp5mfqfvi?}

fjddrZHF{H0l_Fa_Afre_F12v_Uz_Bk5halaqd?}
quoocKSQ{S0w_Ql_Lqcp_Q12g_Fk_Mv5slwlbo?}
txrrfNVT{V0z_To_Otfs_T12j_In_Py5vozoer?}
mqkkyGOM{O0s_Mh_Hmyl_M12c_Bg_Ir5ohshxk?}
imgguCKI{K0o_Id_Diuh_I12y_Xc_En5kdodtg?}
rvppdLTR{T0x_Rm_Mrdq_R12h_Gl_Nw5tmxmcp?}

furryCTF{H0w_To_Hide_F12g_In_In5taller?}
```

D 丢失的文档

E 黑暗

把 8 张图全部丢进 winhex，发现每张图的末尾有 4 个字节是不一样的





8 张图全部组合起来为 ZnVycnlDVEZ7SGVsbG9fSUVORF9Bd0F9，base64 转换一下得到 flag

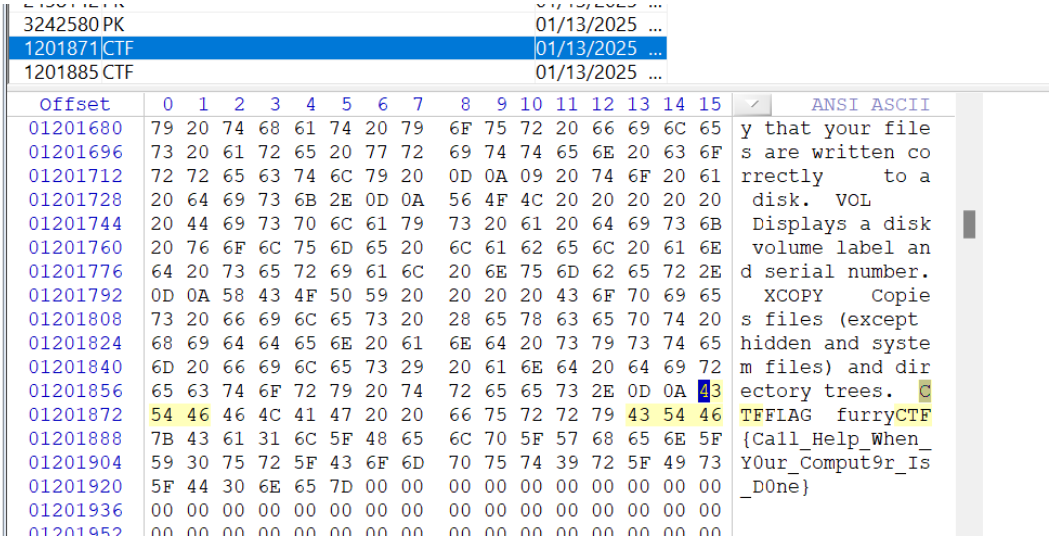
furryCTF{Hello_IEND_AwA}

F 校园浏览器

看评论是 5 年前就有了，但是最后发布是近期，估计是藏 flag 了，果断查看修改记录

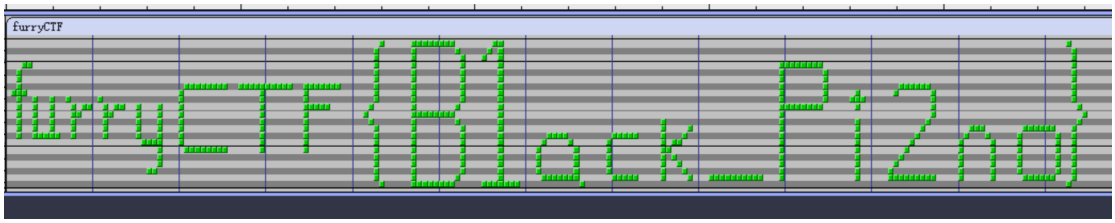
K windows1.0

丢尽 winhex 里搜一下



M 此时无声胜有声

丢到 audacity 里



[Web]

U flag 下载

看题目提示，应该有个附件，只是没挂链接，那就看别的题的附件链接，模仿一下

```
<p>
  <a href="./34990/file/win1.0.img?tid=6728fe9aa325b9e5ba5f9489">
```

构建 payload

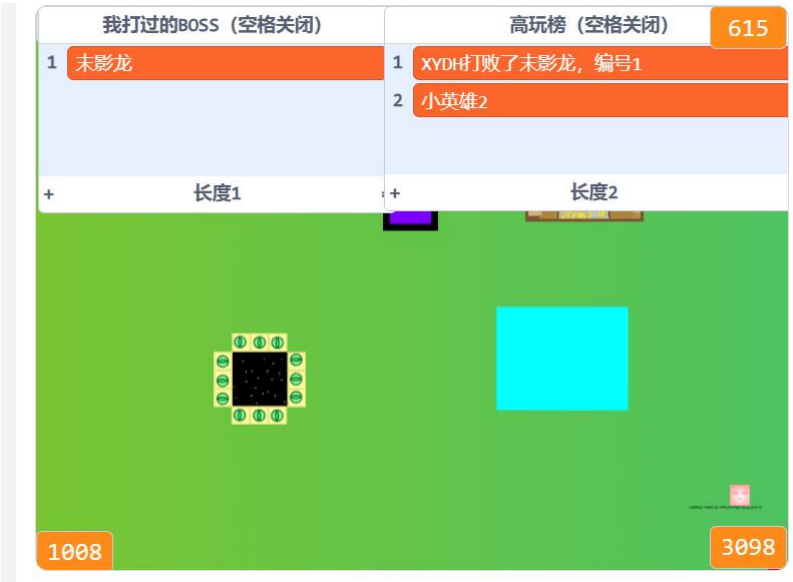
/34977/file/flag.txt?tid=6728fe9aa325b9e5ba5f9489

得到附件，内容要在转码一下，得到 flag

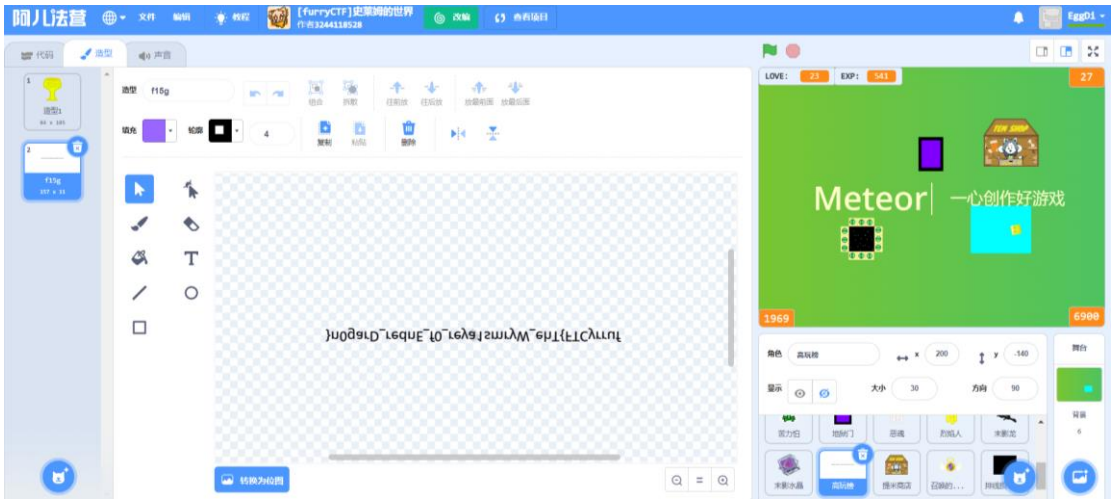
furryCTF{D#n't_Y%u_Kn@w_The_HTML_Re*p0nce}

X 史莱姆的世界

正常过关，稍微分享一下过关技巧，夜晚待在水里可以免受末影人侵害，2 级后后解锁冲击波，M 键使用，杀怪更快，地狱和地狱城堡开启了就去，那边的怪经验多，射击的方向为鼠标中心，杀到 10 级进去末地，用爬行者炸水晶，然后 M 键打龙，留蓝条 等末影人生了用爬行者炸死可以回蓝，稍微走位半小时内能通关。



通关后得到以上界面，原右下角会有个奖杯，字体像素太低看不清，只能另辟蹊径，点击转进设计页，找到奖杯造型，发现 flag

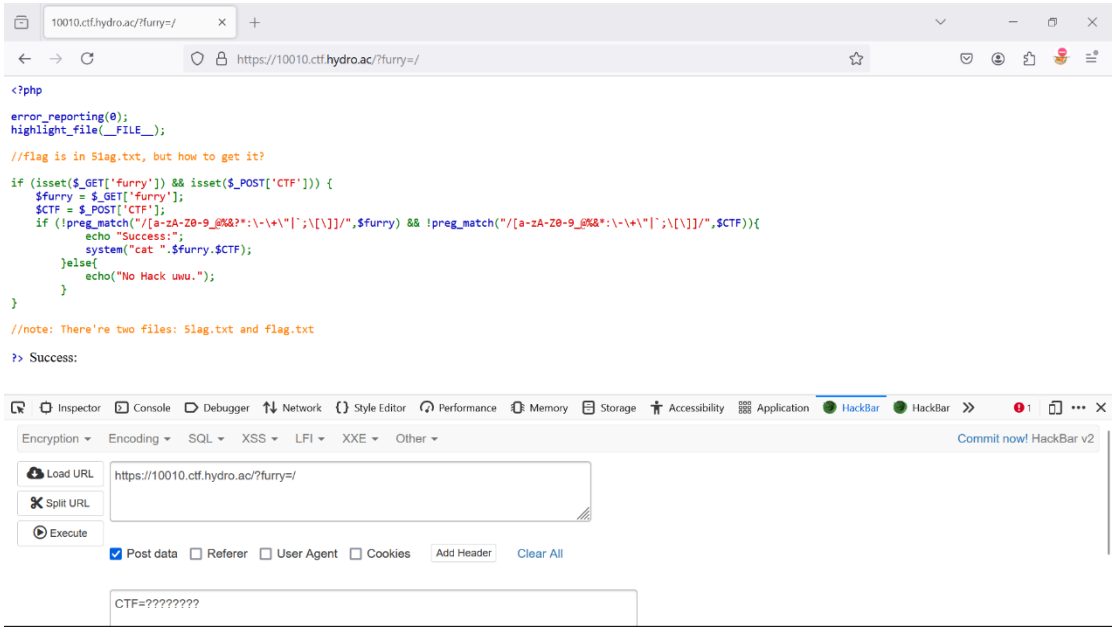


用 python reverse 一下，提交

furryCTF{The_Wyrms1ayer_0f_Ender_Drag0n}

Z 剑走偏锋

Post furry，get CTF，有正则限制，但不影响构造 payload

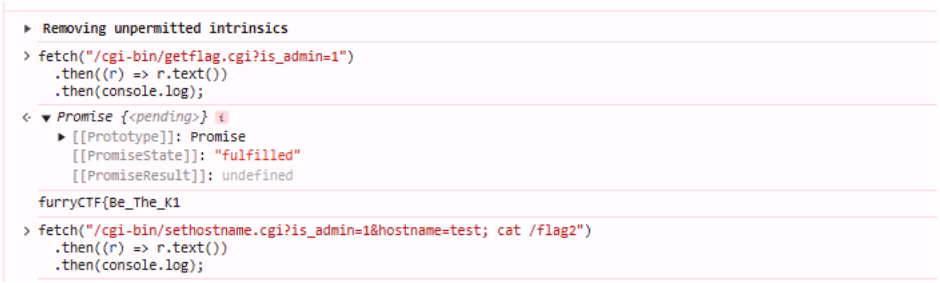


写 wp 时貌似环境异常，flag 没加载出来

furryCTF{Hundred_Secrets_An6_4_Mere_Care1essness}

] 调试窗口 （兼 pwn）

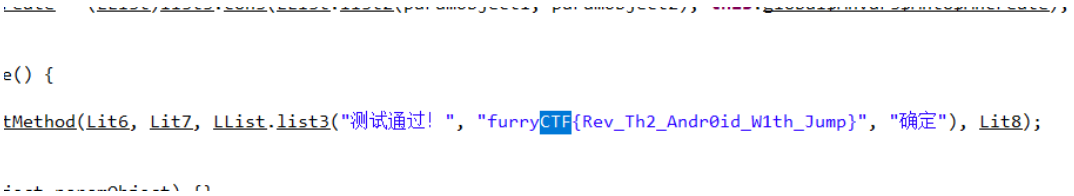
代码审计较长，不附截屏了，重点其实就是有个 popen，然后 admin=1 以及 host 后面可以拼指令，其他的直接在浏览器 console 注 payload 就行



[mobile]

_ 登录

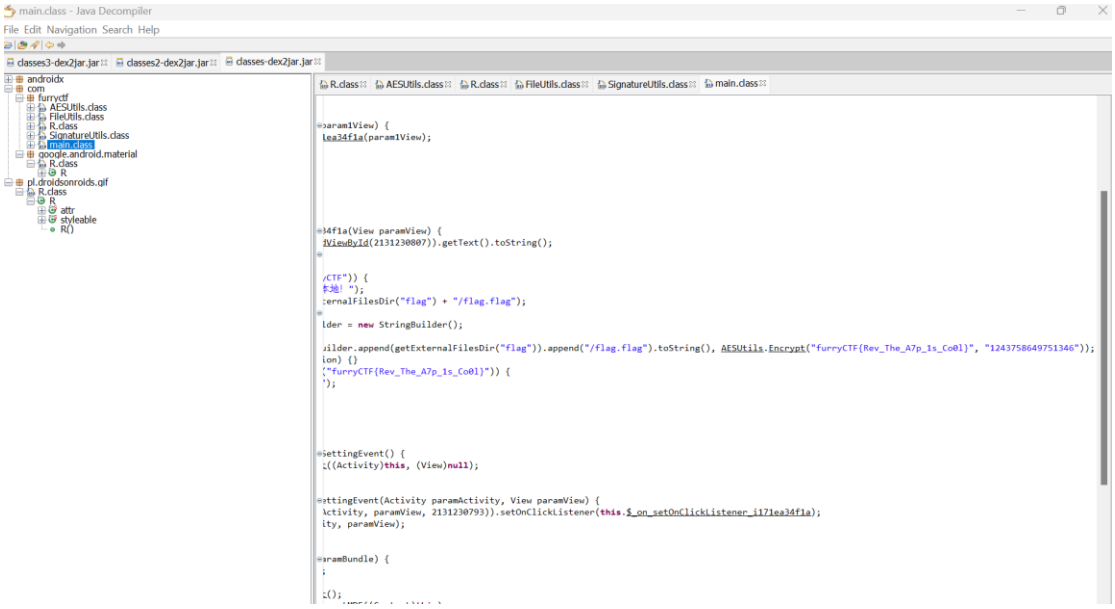
改 zip，反编译，代码审计



‘ 认证系统

前几步改 zip，反编译就不说了，代码审计

Classes 下的 furryCTF-main

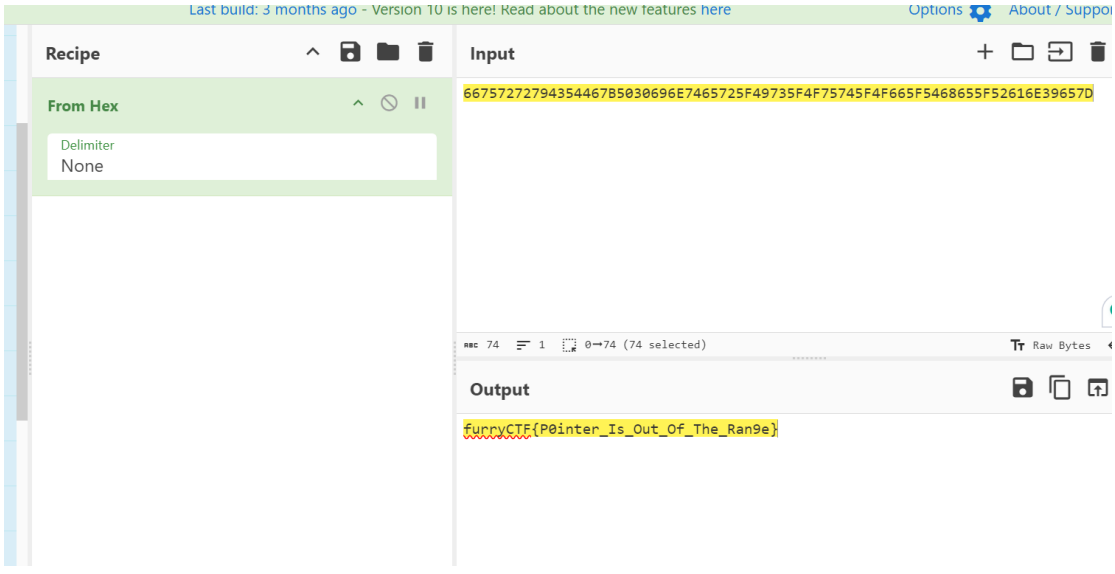


[rev]

b login

丢尽 ida 查看字符串

看到可疑的数字，转十六进制，转字符串得到结果



[crypto]

f 亡羊补牢

每隔 n 位取一个字母，如果当前字母取过了就取下一位（写 wp 的写题的时间差得有点远，不太记得 n 是多少了好像 13 还是 17，师傅们自己试一下吧）

furryCTF{A_New_Interest1ng_Rail_Fence_C1pher}

h MD5

题目都说 md5 了，那就 cmd5，启动

四个字符串就进去匹配一下，分别得到四个单词，拼凑得到 flag

furryCTF{furlary_furbbs_seeyou_again}

j 粗心的猫猫

上脚本

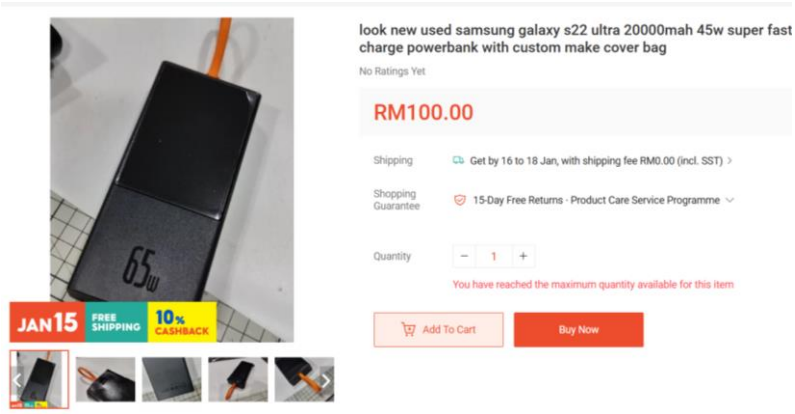
```
import gmpy2
import libnum

e = 65537
c1=1417764517503922911634603040313209923225229115313530740796847201538630396968
n1=3074549153012287940051848662160225605497305792390077116840311063418829412450
c2=2616225154450846689007019196467926428889335392687050302769125495331219155668
n2=3573732341107374111496171426065612539413260680402098416454376398047835410215

n=[n1,n2]
c=[c1,c2]

for i in range(len(n)):
    for j in range(len(n)):
        if(i!=j):
            if(gmpy2.gcd(n[i],n[j])!=1):
                print(i,j)
                p = gmpy2.gcd(n[i],n[j])
                print("p = ",p)
                q = n[i] // p
                print("q = ",q)
                d = gmpy2.invert(e , (p-1)*(q-1))
                print("d = ",d)
                m = pow(c[i],d,n[i])
                print("m = ",m)
                print(libnum.n2s(int(m)))
```

```
0 1
p =  342873543211759555388802552743430819399105092278802461476997495691
q =  896700609855289626547128001485838531980300794067866621906233229231
d =  224212166669082010953961888872886556240799450288690290439215995016
m =  218850620616752632275089946056874286800978532205512300961352968561
b'furryCTF{The_Eas9_RSA_Enc0de_1n_furryCTF}'
1 0
p =  342873543211759555388802552743430819399105092278802461476997495691
q =  104228874226677446063679158775947755721641299298361770343057593709
d =  214755482841496734109058576487697054548899774747510325366163702464
m =  218850620616752632275089946056874286800978532205512300961352968561
b'furryCTF{The_Eas9_RSA_Enc0de_1n_furryCTF}'
```

[hardware]

l Charge

图片搜索，查到以下资料，得知充电宝容量为 20000mah



查询倍思充电宝 65w 20000mAh，找到机型为 PPJL65C

姓名： 充电宝
型号.: PPJL65C|
电池： 锂离子聚合物电池
容量: 5000mAh/14.8V/74Wh(20000mAh/3.7V)
额定容量： 12000mAh（5-3A）
能量转换率：27596

查询“65w 快充 iphone 14 充多久”，发现以下描述

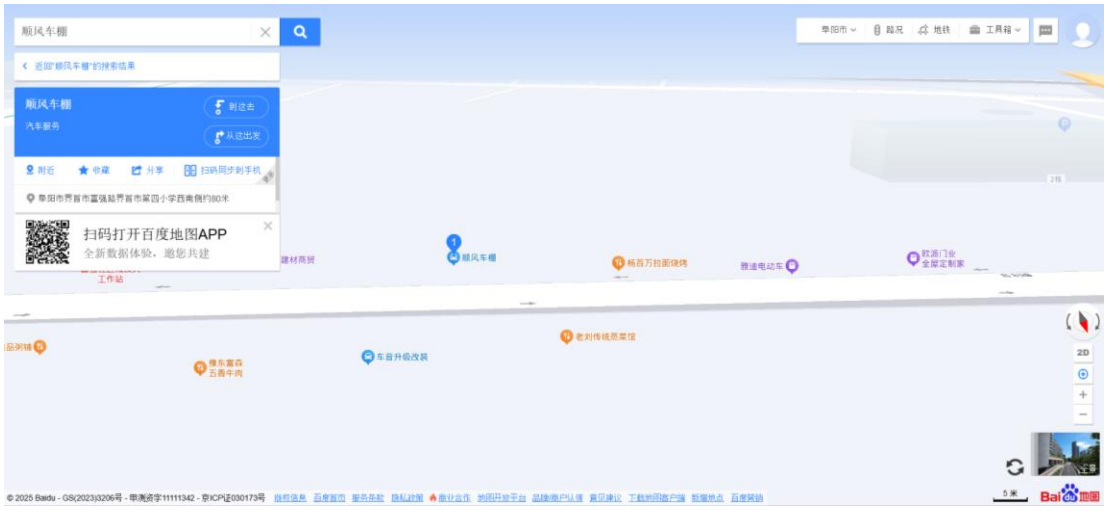
尝试使用 50%电量，提交成功

furryCTF{20000_50_PPJL65C}

[osint]

o 人文风景

百度地图搜索图片中出现的几家店，搜到顺风车棚只有俩个选项，点击第一个，打开来看到对面有家老刘传统蒸菜馆，尝试提交后成功



furryCTF{laoliuchuantongzhengcaiguan}

p 循迹

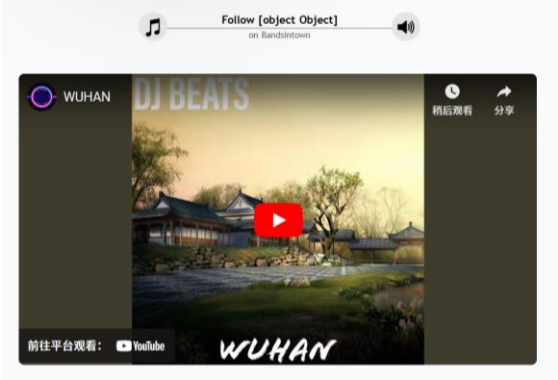
放大 image1,发现右下角写着即墨古城，搜索即墨古城 火锅店

填入第一个发现直接对了

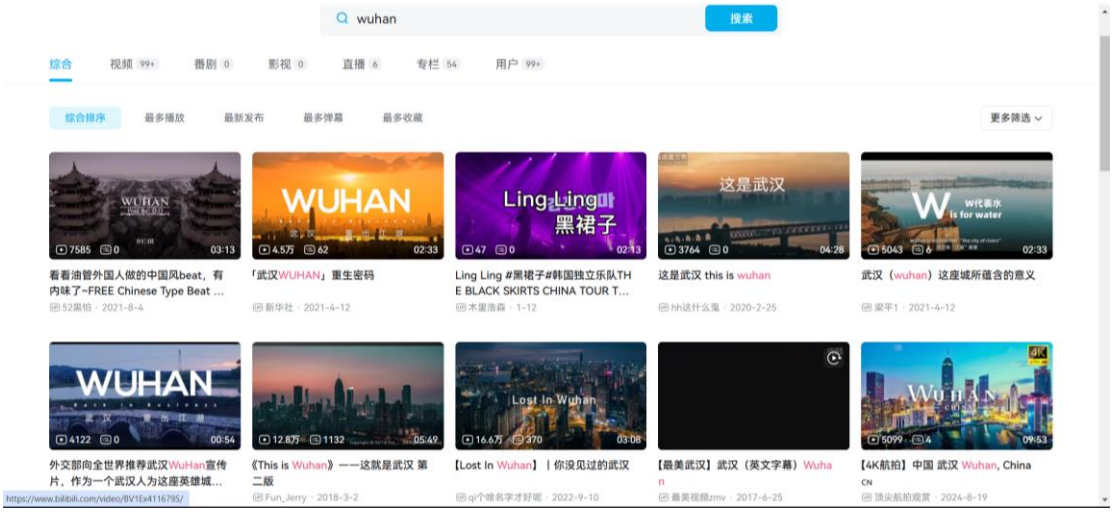
furryCTF{dezhuanghuoguo}

q 神秘影片

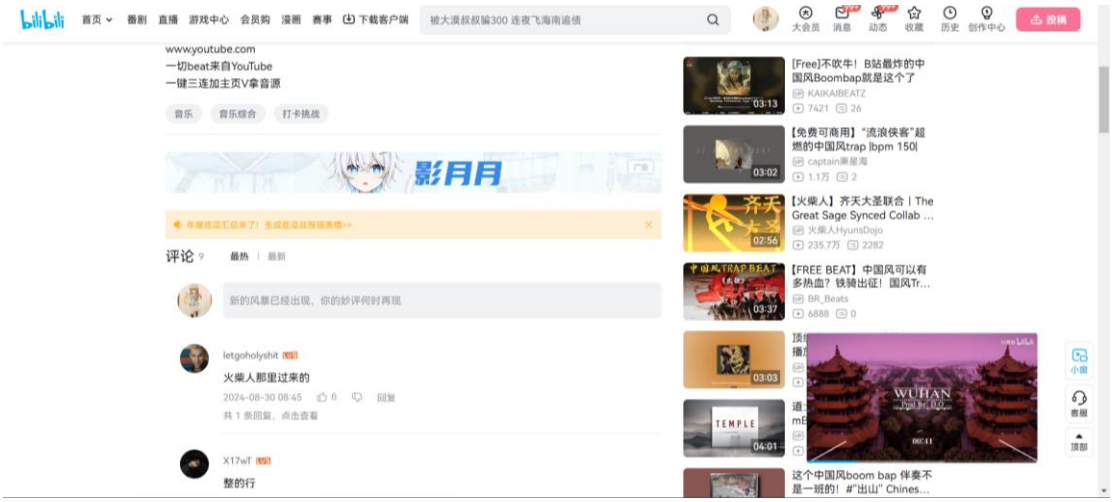
使用 AHA Music 插件，识别到以下歌曲



b 站搜索 wuhan，找到类似的音频，但是时长不对



点进第一个视频，在评论区看见关键词“火柴人”，右边推送区也有火柴人，而且时长居然和题目差不多，果断点开



果然是他，打斗音都有， bv 号在链接后缀，提交成功

furryCTF{BV1Bf4y157pa}

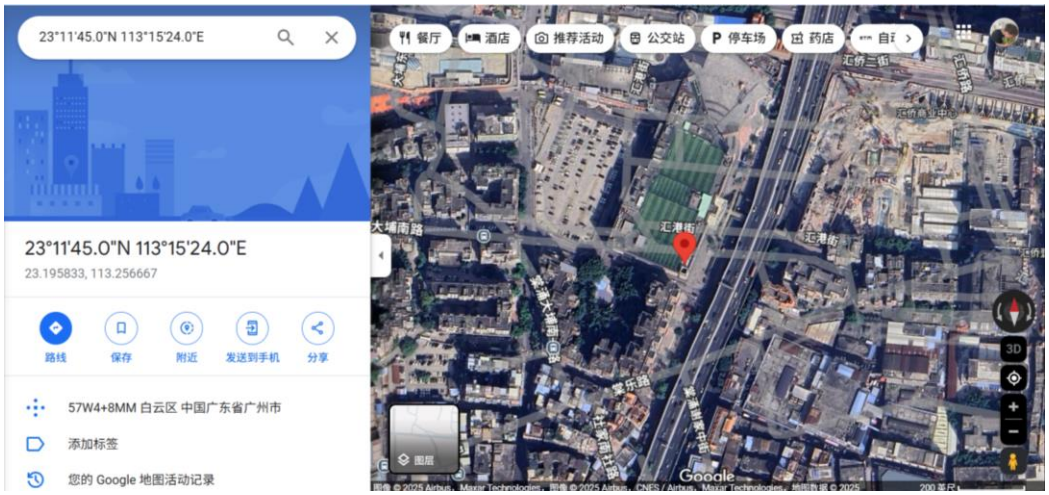
r 出勤!

用 https://exif.tuchong.com/ 查看图片的 exif 信息，得到拍摄的经纬度

GPS

GPSLatitudeRef	North
GPSLatitude	23 deg 11' 45.14"
GPSLongitudeRef	East
GPSLongitude	113 deg 15' 24.74"
GPSAltitudeRef	Above Sea Level

到谷歌地图搜索以上经纬度，查到广东省白云区



使用全国音游地图，定位到广州市白云区，然后一一对比

全国音游地图

白云区

店铺名称	地址
51区动漫游戏主题乐园	白云新城云霄路353号五号停机坪3层L3002N
环游嘉年华金沙洲永旺店	金沙洲沙凤三路1号金沙洲永旺梦乐城4层
环游嘉年华(大玩家)白云万达店	白云新城云城东路501号白云万达广场3层358
曼宗斯同和店	同和大街1号同和金铂广场A座2层A220
天空之城广州嘉禾店	望岗鹤龙二路85号嘉禾金铂天地2层
Kikis其趣同和店	同和大街1号金铂广场A座2层
精空进击社时光汇店	黄边北路152号广州设计之都时光汇3层
天空之城广州百信店	新市棠乐路1,3,5,7号百信广场西区3层XL3019
精灵岛白云江高店	江高夏花三路38号江鼎广场3层
超能量客凯德广场店	白云新城云城西路890号凯德广场云尚3层14/34
精空进击社嘉裕太阳城店	京溪广州大道北1811号嘉裕太阳城2层2059
Top City白云百信店	新市棠乐路1,3,5,7号百信广场西区B1层XB1037

搜索到疯狂牛仔城白云百信店时，发现天花板设计和照片一致

确信该地区就是照片上的地点，按照题目指示和收录机种排序，提交发现不对

全国音游地图

收录机种

机种	版本	台数	价格	机台说明
maimai DX	国行2024	2	3	一台佛山保利店调拨机台，机况一般；一台新机（在靠里一侧），新机没开续关（2024.8.22）
CHUNITHM	华立国行（中二节奏2025）	2	3	新机，可续关 外放声音小，加上旁边太鼓外放声音干扰，建议使用耳机 另请留意，排卡和舞萌一样在机台下方 游玩人数相对来说不是太多
太鼓之达人	虹	1	12	12币3曲，灵敏度不太够蓝要大力敲，虽是新机但小孩拆鼓严重（这个价格完全没有性价比）。
头文字D	激斗	4	4	2p已修复，四台机正常
湾岸MIDNIGHT	SDX+	4	12	有终端机，机况良好，周末人多

点开编辑历史发现有部分机型是在拍摄日期（12 月 1 日 2024 年）之后更新的

全国音游地图

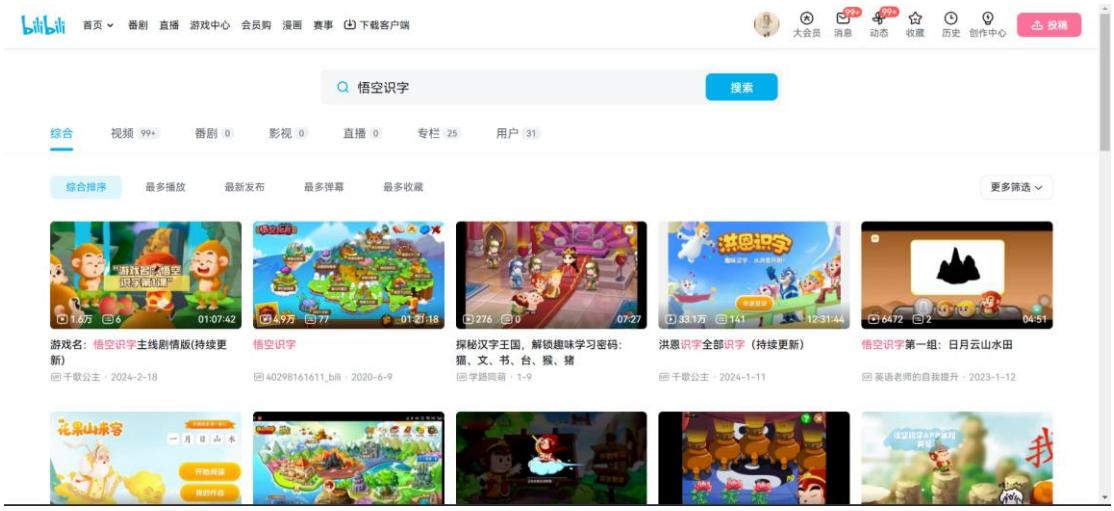
编辑历史

- 头文字D
  Lzhian
  2025-01-10 09:08:23
- 湾岸MIDNIGHT
  Lzhian
  2025-01-02 10:10:17
- 头文字D
  Lzhian
  2025-01-02 10:09:46
- 湾岸MIDNIGHT
  Lzhian
  2024-12-24 01:17:42
- 头文字D
  HNX-13
  2024-12-05 18:08:35
- 更改信息:天空之城没有舞立方秀
  kiq.
  2024-10-18 23:31:04
- 编辑店铺信息
  Linkping
  2024-10-09 09:46:24

按照拍摄日期前的机型排序后提交，成功

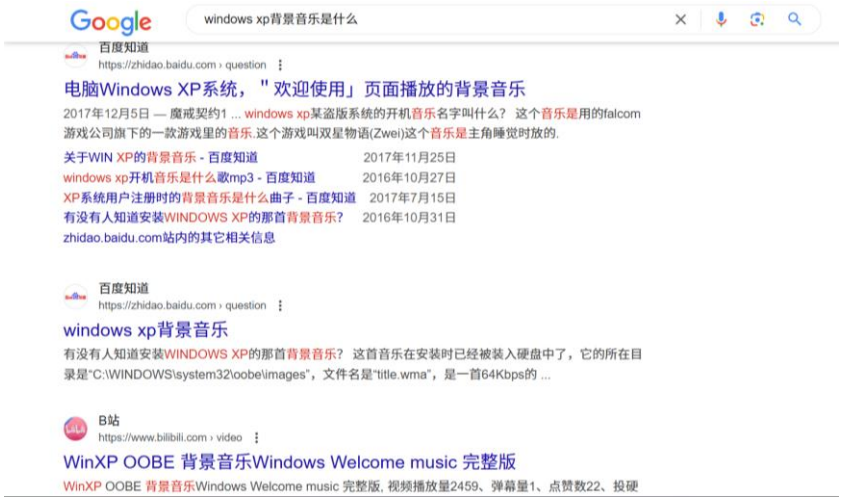
furryCTF{22144-331238}

s 这些东西有什么共同点?



先在 b 站搜索悟空识字，大概听了一下主界面的背景音乐

由于题目的注指到了游戏名称，想说是跟 windows xp 有关的小游戏，搜索无果，然后搜索 windows xp 背景音乐，发现以下关键字：“游戏”



b 站搜索双星物语，发现旋律几乎差不多，果断提交

furryCTF{shuangxingwuyu}

t 个人主页

看题目链接是 gitee，直接 gitee 个人主页改链接访问 cclmsy，在 myblog 下找到 sitemap

```
<?xml version="1.0" encoding="UTF-8"?>
<urlset xmlns="http://www.sitemaps.org/schemas/sitemap/0.9">

  <url>
    <loc>http://www.cclmsy.cc/posts/11f0411.html</loc>

    <lastmod>2023-10-26</lastmod>

    <changefreq>monthly</changefreq>
    <priority>0.6</priority>
```

访问后找到对应主页，开搜

在“关于”的框架栏找到博客框架和托管平台

在旧时光内找到 gitee 关闭日期

furryCTF{Hexo_Vercel_2023-12-14}

u 旅行照片

直接图片搜索就找到了

furryCTF{riyueshuangta}

w 归去

从图片看到俩班车次，G2805 和 G3191，先搜索 G2805 车次，发现 18:12 的发车时间的站名为界首南

G2805次列车（高速），始发站：**石家庄**；终到站：**杭州西**；全程共有19个停靠站：

站序	站名	车次	到达时间	发车时间	耗时	是否当日	停靠时间
1	石家庄	G2805	----	14:39	00:00	当日到达	0分钟
2	邢台东	G2805	15:06	15:09	00:27	当日到达	3分钟
3	鹤壁东	G2805	15:47	15:50	01:08	当日到达	3分钟
4	新乡东	G2805	16:06	16:17	01:27	当日到达	11分钟
5	郑州东	G2805	16:38	16:41	01:59	当日到达	3分钟
6	扶沟南	G2805	17:21	17:23	02:39	当日到达	2分钟
7	周口东	G2805	17:40	17:42	02:58	当日到达	2分钟
8	沈丘北	G2805	17:56	17:58	03:17	当日到达	2分钟
9	界首南	G2805	18:10	18:12	03:31	当日到达	2分钟
10	临泉	G2805	18:22	18:24	03:43	当日到达	2分钟
11	阜阳西	G2805	18:39	18:43	04:00	当日到达	4分钟
12	淮南南	G2805	19:18	19:20	04:39	当日到达	2分钟
13	合肥南	G2805	19:58	20:04	05:19	当日到达	6分钟
14	巢湖东	G2805	20:25	20:27	05:46	当日到达	2分钟
15	芜湖	G2805	20:48	20:50	06:09	当日到达	2分钟

搜索界首南列车时刻表，按照发车时间排序

G2693	高铁	新乡东	08:40	界首南	10:48 (当日)	10:50 (当日)	潮汕	22:44 (当日)
G3101	高铁	郑州东	09:41	界首南	11:05 (当日)	11:07 (当日)	南京南	13:45 (当日)
G3104	高铁	郑州东	09:41	界首南	11:05 (当日)	11:07 (当日)	南京南	13:45 (当日)
G2806	高铁	杭州西	07:13	界首南	11:07 (当日)	11:09 (当日)	石家庄	14:12 (当日)
G7723	高铁	界首南	12:03	界首南	-	12:03 (当日)	安庆	15:29 (当日)
G7733	高铁	界首南	12:47	界首南	-	12:47 (当日)	芜湖	15:34 (当日)
G1964	高铁	温岭	06:39	界首南	13:45 (当日)	13:47 (当日)	郑州东	15:22 (当日)
D3356	动车	杭州西	09:52	界首南	14:19 (当日)	14:21 (当日)	太原南	19:20 (当日)
G7499	高铁	界首南	15:11	界首南	-	15:11 (当日)	温州南	22:02 (当日)
G1963	高铁	郑州东	13:56	界首南	15:33 (当日)	15:35 (当日)	温岭	21:49 (当日)
G1577	高铁	北京西	10:48	界首南	16:12 (当日)	16:15 (当日)	阜阳西	16:41 (当日)
G2808	高铁	宁波	12:56	界首南	17:53 (当日)	17:55 (当日)	石家庄	21:48 (当日)
G7275	高铁	界首南	17:56	界首南	-	17:56 (当日)	上海	21:49 (当日)
G2805	高铁	石家庄	14:39	界首南	18:10 (当日)	18:12 (当日)	杭州西	22:26 (当日)
G1578	高铁	阜阳西	17:45	界首南	18:11 (当日)	18:13 (当日)	北京西	23:08 (当日)
G3191	高铁	焦作	15:35	界首南	18:27 (当日)	18:29 (当日)	温岭	23:30 (当日)
G7735	高铁	界首南	19:13	界首南	-	19:13 (当日)	黄山北	22:36 (当日)
G3106	高铁	杭州东	15:48	界首南	19:50 (当日)	19:52 (当日)	新乡东	21:43 (当日)

排在 G2805 前面的班次钟点站为上家海站，尝试后提交成功

furryCTF{shanghaizhan}