

# Task 1

选择Task 1.2 ZJUCTF2023 的 NATO26

## flag:

- flag: ZJUCTF{Y0u\_rE@1Ly\_Kn0W\_encODIng}
- 比赛平台通过截图:

## 解题思路:

1. 我们拿到了一串乱码, 猜测他是之前提到的情形

5: 先用 GBK 解码 UTF-8 编码的文本, 再用 UTF-8 解码前面的结果。根据提示, 我们将这段文本先通过编码保存 (Save with Encoding), 选择 GBK, 再选择"通过编码重新打开", 选择 UTF-8, 得到如下结果:

原理类似贝斯五十? ? ? 贝斯二十? ? ? 码其内? ? 为喝彩声帕帕利马魁北克回音查理均匀帕帕回音祖鲁人狐步探戈?

2. 再根据这个题目, NATO26 的提示, 这段话应该是北约字符的加密。前面的

原理类似贝斯五十? ? ? 贝斯二十? ? ? 码其内? ? 为 是提示, 告诉我们这段话进行了 Base26 加密, 所以只看后面的文本, 对照北约字符表, 解密的得到的结果是:

BPLQECUPEZFTSUJJQDZWGGXBOXZMEUZSDHVGKVMNEVWSKDKICMAIUOB

• Tips:

- 部分的字符, for e.g. 拉 一下子翻不到合适的字符。但是可以发现这三个字符: ?拉 经常一起出现。然后发现在这个密文的后面, 出现了一段类似的 ? ? ? 塞拉? ? ? , 联想到 Silicon → S 所以明文就给了S
- 均匀→Uniform→U, wiki pedia里写的是“制服”, 一时间还没想到

3. 最后写了一个脚本 decoding.py, 来获得明文

脚本如下:

```

s='BPLQECUPEZFTSUJJQDZWGGXBOXZMEUZSDHVGKVMNEVWSKDKICMAIUOB'
output=0
for i in range(len(s)):
    output=output*26+(ord(s[i])-65)
# convert to bytes, then group -> hex
anss=bin(output)[2:]
while len(anss)%8!=0:
    anss = '0' +anss # make sure can -> hex
ans=''
for i in range(0,len(anss),8):
    byte=anss[i:i+8]
    num10=int(byte,2)
    ans+=chr(num10)
print(ans)

```

输出:

所得的 ZJUCTF{Y0u\_rE@1Ly\_Kn0W\_encODIng} 即是flag

## Challenge 3: OSINT

### 3.1 Task 1: 45gfg9's easy OSINT

1. 所在位置推测:

思路:

简单地学习了一下韩语输入法, 在手机上打出了"봉 은 사", Google Map, 奉恩寺

看了一下简介:

发现可以在原照片中简单的看到弥勒佛头像的一个头

由此可以断定确实是奉恩寺景区入口 (而且车非常拥挤, 和旁边这条路的车流量差好多, 看起来就是景区入口)

街景空降这个地方, 会发现一个一模一样的上坡, 也是一个类似的路口

路牌想必在路口的前面一些的位置，于是继续后退

在这个角度要素就齐全了，有一样的路牌，高楼（由于是18年街景，当时矮的那幢楼还不叫“SPARKPLUS”，但是高度一致

仔细看路牌，对照文字，确认地点就是在这里

缩略图：

放大一点：

2. 右半边内容：

- Olympic Expwy
- Seoul Medical Center

思路：

谷歌地图讲的很清楚了……【嘿嘿】

## 3.2 Task 2: pumpk1n's real OSINT

四个问题的答案：

1. 赛事名称：第八届XCTF国际网络攻防联赛总决赛
2. 航班号：GS6508
3. 航班大致时间：16：05-18：50
4. 江中岛的位置：

**解题思路：**

主要知道它是CTF比赛，然后打开这张图的属性发现了拍摄时间：

发现拍摄时间是2024.6.23，于是找一找有没有这附近的赛事，合理推测pumpk1n老师应该参加的是这里提到的**比赛**，一个个搜x

搜到了一条新闻 <https://baijiahao.baidu.com/s?id=1802790751868414758&wfr=spider&for=pc>，这个时间段，合理推测6.23闭幕，pumpk1n老师回杭

下面寻找是什么航班

谷歌搜图，搜到机尾对应的航空公司 [https://m.thepaper.cn/newsDetail\\_forward\\_7231376](https://m.thepaper.cn/newsDetail_forward_7231376)

对照知道它是天津航空：

原图：

帖子：

下面搜天津航空的网，刚好发现了15：45-18：30的，成都飞杭州的航班

<https://www.tianjin-air.com/flights/results/TFU-HGH-240708-100-0>

时间：18：30 和我们看到的拍摄时间18：32 不谋而合（可能航班有延误

这个时候由于飞机已经脱离云层降落了，所以大概15分钟左右着陆，所以推测就是 16：05-18：50

由于这是降落时拍的照片，推测这是萧山机场附近，所以谷歌地球和照片对应一下形状

可以看到这里红框对应的岛的形状，以及山的位置以及黄框的平原都是一一对应的，所以确定了江中岛的位置✓