

张万森，下雪了-WP

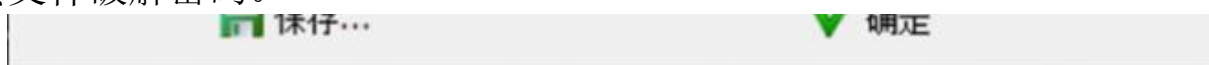
出题人：DOUBL3SEV3N

学校：大理大学

考点：SNOW 隐写，字典爆破，base64 多次编码

解题步骤：

下载附件后得到一个压缩包和一个字典文件 dic.txt。压缩包里面的 txt 文件需要密码，dic.txt 爆破压缩包密码。使用 ARCHPR.exe 字典文件破解密码。



得到压缩包里面的文件密码：dldxwlaqXH

tip.txt 里的密文是经过 base64 进行 45 次编码后得到的，对这段密文进行 45 次 base64 解密，脚本如下：

```

import base64
Sstr=''
with open('tip.txt', 'r', encoding='UTF-8') as f: #打开 tip.txt 文件
    Sstr="".join(f.readlines()).encode('utf-8')
src=Sstr
while True:
    try:
        src=Sstr
        Sstr=base64.b64decode(Sstr) #解码
        str(Sstr,'utf-8')
        continue
    except:
        pass
    break
with open('result.txt','w', encoding='utf-8') as file: #写入明文
    file.write(str(src,'utf-8'))
print('ok')

```

得到明文密钥：ISCTFZ0Z3

查看 flag.txt，可以看到有信息被隐藏起来了，不难发现这是 SNOW 隐写，所以眼见不一定为实，这里的 flag 是迷惑人的，真正的 flag 藏匿在 flag.txt 文件中。解密的密文就是刚刚得到的 ISCTFZ0Z3。

解密如下：

```
SNOW.EXE -C -p "ISCTFZ0Z3" 文件名
```

这样才能得到真正的 flag，如下：

```

C:\Users\86198\Desktop\challenge\isctf2023出题人\张万森，下雪了>SNOW.EXE -C -p ISCTFZ0Z3 flag.txt
ISCTF {34da-a87s-sk87-s384-3982-398233}
C:\Users\86198\Desktop\challenge\isctf2023出题人\张万森，下雪了>

```