加密后的企业数据

发表于 2021-01-25 更新于 2021-02-16 分类于 Challenge ， 2020 ， 工业信息安全技能大赛 ， 湖州站
Challenge | 2020 | 工业信息安全技能大赛 | 湖州站 | 加密后的企业数据

点击此处获得更好的阅读体验

WriteUp来源

来自MO1N战队

题目描述

> *工厂内部转发了一个文件，被检查后发现进行传输了企业敏感数据信息，您能帮助检查出传输的企业关键数据么？Flag格式为：flag{}. Hint：获取到的rar中提示了密码生成方式，最后隐写方式为：0宽度隐写*

题目考点

解题思路

拿到zip压缩包发现无法打开

查看十六进制 符合压缩包的特征，文件头的四字节符合zip特征，但往后符合RAR文件特征

修改文件头后保存rar格式

文件存在密码，压缩包的注释中有给出密码生成方式

编写解密脚本

```
import hashlib

def md5(s):
    return hashlib.md5(s.encode(encoding='GB18030')).hexdigest()

for i in range(0,9999999):
    pwd = str(i).rjust(7, '0')
    if "747fa0eb44e6ed5a349497" in md5(pwd):
        print(pwd)
```

得到密码5546023

打开压缩包后发现

打开16进制发现不可显字符串，看到很多0宽度字符，符合0宽度隐写的特征

编写解密脚本

```python
#!/usr/bin/env python3
#coding: utf-8
import zwsp_steg
# pip3 install zwsp-steg-py

with open("flag.txt", "r") as f:
    flag = f.read()
decoded = zwsp_steg.decode(flag)
print(decoded)
# b5e6a6572761cc9c5d8222682fdf5802
```

Flag

```
flag{b5e6a6572761cc9c5d8222682fdf5802}
```


 # Challenge # 2020 # 工业信息安全技能大赛 # 湖州站
Modbus协议分析
某工控固件分析