组态软件安全分析

发表于 2021-02-16 分类于 Challenge ， 2019 ， 工业信息安全技能大赛 ， 深圳站
Challenge | 2019 | 工业信息安全技能大赛 | 深圳站 | 组态软件安全分析

点击此处获得更好的阅读体验

WriteUp来源

https://xz.aliyun.com/t/5960

题目描述

> *一些组态软件中进行会配置连接很多PLC设备信息。我们在SCADA工程中写入了flag字段，请获取该工程flag*

题目考点

- *力控组态PCZ格式分析*

解题思路

解压附件，发现得到一个.PCZ的文件，用记事本打开发现文件头为PK，于是将.PCZ的文件后缀改为.zip，解压后得到一个演示工程的文件夹，里面包含了很多文件，如图所示：

题目表明Flag就在文件夹中的某一个文件中，一个个打开审计过于麻烦，可以利用linux系统的grep指令，帮助我们在文件夹中查找指定关键字，在演示工程的文件夹中，使用指令grep -r "flag" ./进行搜索，最终得到Flag，

Flag

```
1 flag{D076-4D7E-92AC-A05ACB788292}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2019/工业信息安全技能大赛/深圳站/3m1mS2soi5uQkXSxxXcGnA.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2019 # 工业信息安全技能大赛 # 深圳站
工控蜜罐日志分析
工业协议分析2