S7ccoomm

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 | S7ccoomm

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

> *某工程师在工作中发现有大量来自于某IP对PLC的流量，请尝试分析并找出其隐藏的内容。flag格式为：flag{}。*
> *Hint：协议分析SessionClientRID格式后四位，拼接后可获取特定的文件信息*

题目考点

解题思路

Flag

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/工业信息安全技能大赛/湖州站/h65fnBjfN16mREMRLbi3Uw.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 # 2020 # 工业信息安全技能大赛 # 湖州站
工控协议数据分析
Modbus协议分析