ICS TRITON

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 ， 石家庄站
Challenge | 2020 | 工业信息安全技能大赛 | 石家庄站 | ICS TRITON

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

> *某工控系统受到了来自境外的攻击，因为及时干预未造成更严重的损失，工作人员在SIS 工程工作站上发现了一个可疑文件，流量监控系统也捕获到了一部分攻击流量。试根据已有的条件获取攻击攻击者隐藏在流量中的关键信息。flag格式为：flag{}。*

题目考点

解题思路

Flag

```
1 flag{cb677d72f507b26cb3326db15422ee3e}
```

- ***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/石家庄站/6BwWHmQEFk1bFkFmCndUid.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 # 石家庄站
隐藏的木马文件
西门子PLC协议分析