2

发表于 2021-08-30 分类于 Challenge， 2021， 工业信息安全技能大赛， 巡回赛-兰州站
Challenge | 2021 | 工业信息安全技能大赛 | 巡回赛-兰州站 | 02

点击此处获得更好的阅读体验

WriteUp来源

来自M01N战队

题目描述

> *某工厂怀疑被黑客入侵，工程人员在分析西门子传输协议时，截获一段报文如下：0300002402f080320100000009000e00050501120a10010001000083000029000300010 1 请解读协议内容，并准确的拿到返回值，返回值即为flag，flag形式为flag{}。*

题目考点

- *流量分析*
- *S7Comm协议*

解题思路

利用S7Comm协议的脚本将该段报文发送至S7Comm的服务器端（PLC-SIM），wireshark抓取返回报文，报文中的payload即为flag

Flag

```
1 flag{0300001602F0803203000000090002000100000501FF}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2021/工业信息安全技能大赛/巡回赛-兰州站/3PPVQd6MGniVb7pGL54CQv.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 # 2021 # 工业信息安全技能大赛 # 巡回赛-兰州站
11
10