

S7

发表于 2021-09-01 分类于 [Challenge](#) , [2021](#) , [工业信息安全技能大赛](#) , [巡回赛-杭州站](#)
[Challenge | 2021 | 工业信息安全技能大赛 | 巡回赛-杭州站 | S7](#)

[点击此处](#)获得更好的阅读体验

WriteUp来源

来自Venom战队

题目描述

工业协议中存在异常数据。请通过流量中的数据找寻flag, flag形式为flag{}。提交时请提交括号内内容。

题目考点

- 流量分析
- S7Comm协议

解题思路

过滤s7comm-plus.data.function == createobject, 发现有写操作

□

添加过滤条件s7comm-plus.data.opcode == 0x31, 筛选写操作数据

□

得到字符串ZmxhZ3s5d3pLc0x0bVdmWVduTk00fQ

Base解密得到flag

Flag

```
1 flag{9wzKsLtmWfYWnNM4}
```

- 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-杭州站/mJg7zCJ4CgOiDCWgwmYShU.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-杭州站](#)
[Industry_noaCry](#)
[三句话让PLC为你吐FLAG](#)