



S7Common

📅 2021-09-05 | 📁 Challenge , 2021 , 第七届全国工控系统信息安全攻防竞赛 , 四类

Challenge | 2021 | 第七届全国工控系统信息安全攻防竞赛 | 四类 | S7Common

[点击此处](#)获得更好的阅读体验

WriteUp来源

来自 毕方安全实验室 战队

题目描述

查看工控数据包，获取隐藏的信息。flag格式:flag{xxxxxx}

提示信息

无

题目考点

- 流量分析
- 西门子S7Comm协议

解题思路

下载附件后使用Wireshark打开

过滤出 `s7comm` 包，之后进行TCP follow发现flag字样



使用条件 `s7comm && ip.addr==192.168.1.200 && s7comm.param.func==0x04` 过滤出相关数据



逐一按地址检索得到:

```
1  45-49flag{
2  50 U  190
3  51 2  198
4  52 F  1a0
5  53 s  1a8
6  54 d  1b0
7  55 _  1b8
8  56 G  1c0
9  57 V  1c8
10 58 k  1d0
11 59 X  1d8
12 60 1  1e0
13 61 9  1e8
14 62 r  1f0
15 63 _  1f8
16 64 2  200
17 65 7  208
18 66 h  210
19 67 E  218
20 68 Y  220
21 69 K  228
22 70 }
```

根据题目提示去掉不可显示字符即可获得flag

Flag



```
1  flag{U2Fssd_GVkX19r_7hEEYK}
```

本文作者： CTFHub

本文链接： <https://writeup.ctfhub.com/Challenge/2021/第七届全国工控系统信息安全攻防竞赛/四类/iYGfxF9Cf4chNPy9DTQynb.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](#) [# 第七届全国工控系统信息安全攻防竞赛](#) [# 四类](#)

[← similarPic](#)

IEC104 [→](#)

© 2019 – 2022 CTFHub

由 [Hexo](#) & [NexT.Gemini](#) 强力驱动