#### **CTFHub**

Writeup

## **S7**

 □ 2021-09-01 | □ 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。

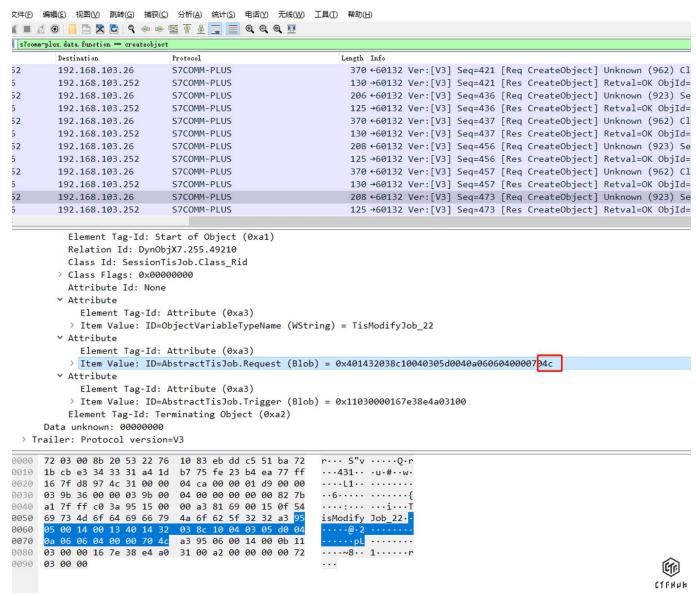
## 题目考点

- 流量分析
- S7Comm协议

### 解题思路

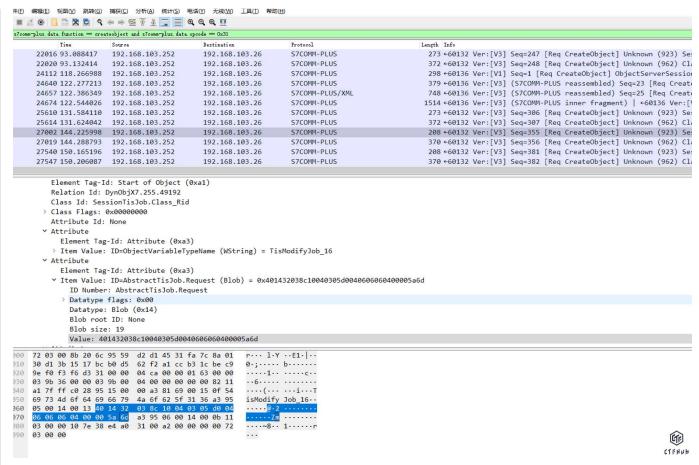
过滤 s7comm-plus.data.function == createobject , 发现有写操作

2023/7/24 21:31 S7 | CTFHub



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

2023/7/24 21:31 S7 | CTFHub



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/mJg7zCJ4CgQiDCWgwmyShU.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 >

2023/7/24 21:31 S7 | CTFHub

© 2019 – 2022 **CTFHub** 

由 Hexo & NexT.Gemini 强力驱动