



Reverse analysis

📅 2021-09-01 | 📁 Challenge , 2021 , 工业信息安全技能大赛 , 巡回赛-上海站

Challenge | 2021 | 工业信息安全技能大赛 | 巡回赛-上海站 | Reverse analysis

[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

组态王6.55的工程文件包含数据的采集的功能，怀疑组态工程文件中隐藏隐蔽信息，请对工程文件逆向分析，找出其中的flag。

题目考点

- SSRF
- OpenPLC RCE

解题思路

解压工程后使用grep递归寻找flag关键词，最终在pic00004.pic中匹配到，提取该文件中所有明文字符，找到flag

```
+ Reverse analysis grep -r "flag" .  
Binary file ./pic00004.pic matches  
+ Reverse analysis strings ./pic00004.pic | grep flag  
//flag{KingviewSmartMeter}  
+ Reverse analysis
```

Flag



```
1 flag{KingviewSmartMeter}
```

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-上海站/x6rKMKUUyVHjF9jtp9DVkp.html>

版权声明： 本博客所有文章除特别声明外，均采用 [CC 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-上海站](#)

< Attachment

Login >

© 2019 – 2022 ❤ CTFHub

由 [Hexo](#) & [NexT.Gemini](#) 强力驱动