#### **CTFHub**

Writeup

## Q

# 隐藏的工程

 □ 2021-09-01 | □ Challenge , 2021 , 工业信息安全技能大赛 , 线上赛-第一场

 Challenge | 2021 | 工业信息安全技能大赛 | 线上赛-第一场 | 隐藏的工程

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

老代凭借多年工业企业运维经验,发现ICS工程师的工作电脑中有一张可疑的工艺图。在对图片进行分析时,发现其中存在异常信息,您能从中找到flag吗? flag格式为:flag{}

## 题目考点

### 解题思路

F5隐写 https://github.com/matthewgao/F5-steganography

```
D:\CTF\ctftools\lalalatools\stego\F5\f5-steganography\tests>java -jar f5.jar x -e 1.txt gcwj.jpg -p ICS
Huffman decoding starts
Permutation starts
6064128 indices shuffled
Extraction starts
Length of embedded file: 35 bytes
(1, 127, 7) code used
```

提取出来一个蓝凑云连接: https://wwr.lanzoui.com/ilMaiqcpaxg

### 是kingview 6.55工程文件

```
4E CC 60 AB 4E CC 60 AB 4E CC 60 00 C2 02 00 20

EA 63 6F 6D 64 65 76 2E 64 61 74 00 B5 CD B3 2D êcomdev.dat.µî -

6B 69 6E 67 76 69 65 77 36 2E 35 35 5C 63 6F 6D kingview6.55\com
64 65 76 2E 64 61 74 00 46 CO 00 82 71 17 5D CD dev.dat.FÀ.,c.;

AB BA DC 00 00 00 00 2C E9 12 00 82 71 17 5D 58 «°Ü....é...g.]X
```

### 打开该工程后发现有个flag用户



利用星号密码查看器查得到明文密码,密码即为flag





Flag

1 flag{fAx9AKoqNgv3dfHg}

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/线上

赛-第一场/dn6oRRe9hfWDv85ZvtwKRL.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
♣ # 线上赛-第一场

< 工控现场里异常的文件

工控安全异常取证分析 >

© 2019 – 2022 **CTFHub** 

由 Hexo & NexT.Gemini 强力驱动