

虚拟PLC

发表于 2021-02-16 更新于 2021-02-17 分类于 [Challenge](#) , [2019](#) , [工业信息安全技能大赛](#) , [成都站](#)
[Challenge | 2019 | 工业信息安全技能大赛 | 成都站 | 虚拟PLC](#)

[点击此处](#)获得更好的阅读体验

WriteUp来源

[纵横网络靶场社区](#)

题目描述

虚拟PLC是基于组态软件的仿真系统实现的原理，在于PLC内部各种继电器的状态与组态软件数据库中数据的链接以及该数据与计算机界面上图形对象的链接。通过修复该文件，分析虚拟PLC工作原理并发现文件中隐藏的flag。

题目考点

- 文件修复
- 西门子PLC编程软件
- PLC仿真

解题思路

先通过西门子S7-PLCSIM 仿真软件，生成一个*.plc 的仿真程序文件，使用正常文件的文件头对题目附件进行修复。

使用S7-PLCSIM 打开修复好的*.PLC 文件，

使用西门子STEP7 编程软件连接虚拟PLC 并从中读取程序，最后可以在DB 块中对数据

进行转码，最后得到flag

□

不过最后千辛万苦解出来的答案，竟然直接就明文显示在文件里面。何必费时间绕这么大一圈，没达到知识点考察的目的

□

Flag

```
1 flag{myfiletypeisplcsim}
```

- 本文作者：CTFHub
- 本文链接：<https://writeup.ctfhub.com/Challenge/2019/工业信息安全技能大赛/成都站/6F6usz17ZtaKfCF6Q2FciZ.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](#) [#2019](#) [#工业信息安全技能大赛](#) [#成都站](#)

[AB协议分析](#)

[工业梯形图分析2](#)