

智能变电站设备异常诊断

发表于 2021-01-25 更新于 2021-02-16 分类于 [Challenge](#) , [2019](#) , [工业信息安全技能大赛](#) , [哈尔滨站](#)
[Challenge](#) | [2019](#) | [工业信息安全技能大赛](#) | [哈尔滨站](#) | [智能变电站设备异常诊断](#)

[点击此处](#)获得更好的阅读体验

WriteUp来源

<https://www.cnpanda.net/ctf/415.html>

题目描述

在电力安全巡检工作中，发现了一个110Kv变电站存在运行异常，经过初步分析问题来源可能是线路智能终端设备。通过分析工作人员导出的变电站基础配置信息文件，分析存在问题根源。flag格式{}

题目考点

- zip文件
- 凯默scd分析软件kscd文件

解题思路

一眼看出题目将ZIP文件头前四个字节倒序了，翻转过来即可解压

□

得到dcs.dcs文件

□

这其实是凯默scd分析软件的kscd文件，文件头还加了两字节垃圾数据。出题人将所有的00都修改为了20，导致文件无法被凯默scd软件正常解析，因此只能从字符串中寻找规律。

□

然后纯粹靠眼力，使用正则表达式将其筛选出来，得到flag

Flag

```
1 flag{scdisbad}
```

- 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/哈尔滨站/ikYmvFFtctwnYzraT2qs4f.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](#) [#哈尔滨站](#)

[协议分析又来了](#)

[黑客的大意](#)