

2021CTF工业信息安全技能大赛-工控梯形图分析2

原创夜白君于 2021-07-05 09:18:41 发布1733收藏4

版权

分类专栏:2021工业信息安全技能大赛-CTF

文章标签:信息安全unctl渗透测试

2021工业信息安全... 专栏收录该内容

36 订阅24 篇文章

订阅专栏

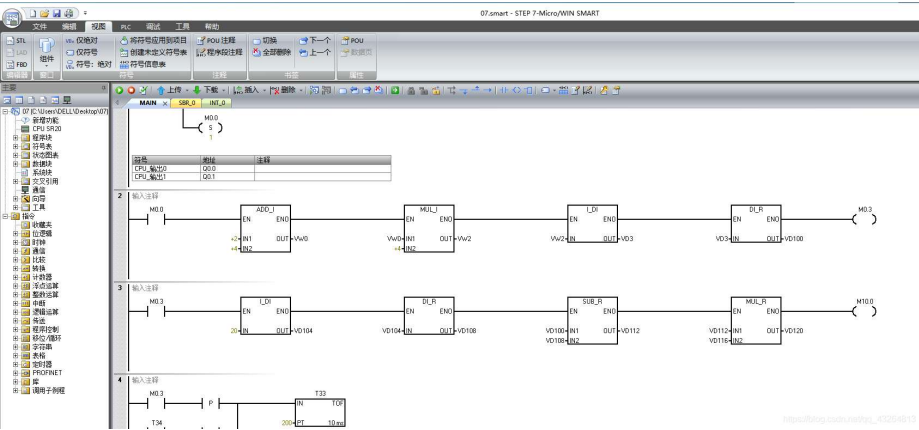
2021CTF工业信息安全技能大赛-工控梯形图分析2

小王是工厂的一名工程师，每天的工作是启动设备进行加工，设备一共进行两次加工。设备在运转过程中突然停止工作，打开梯形图发现其中两个数值丢失，请帮助小王填补数值VD200与VD300，flag为VD200加上VD300。flag格式为flag{VD200_XX_VD300_XX}。

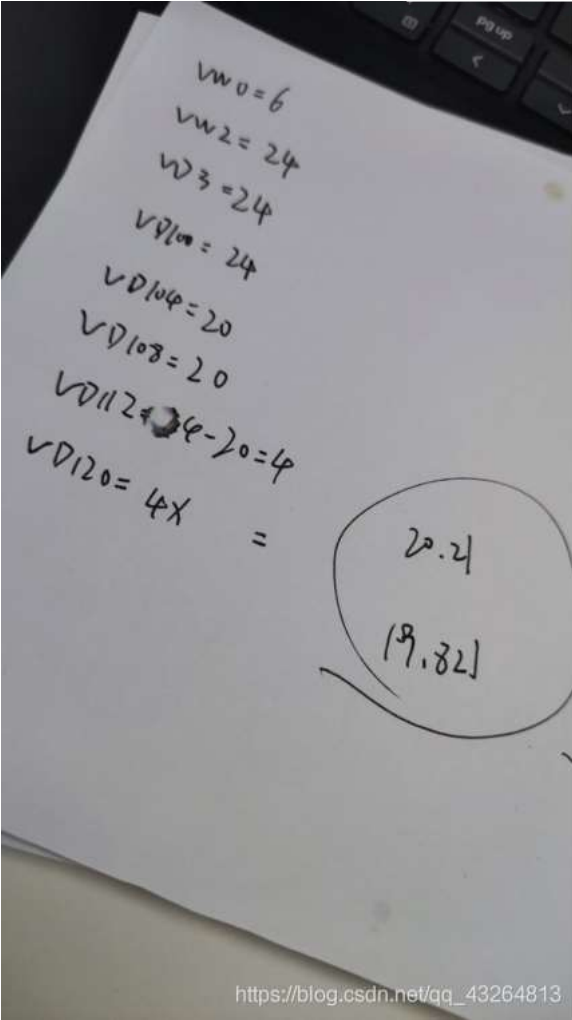
使用工具：STEP 7-MicroWIN SMART

解题步骤：

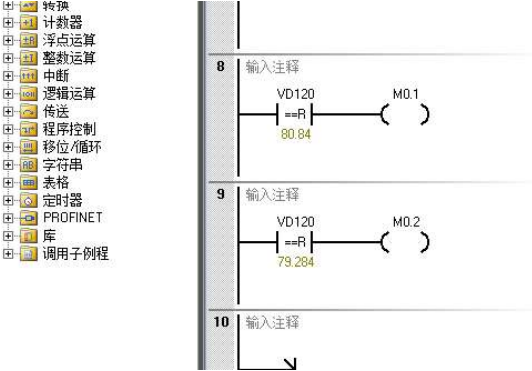
1.使用工具打开工程图查看；



2.手动计算出运行过程各个点位值；



3.分析工程图vd120两次输入值，根据两个值可计算出两次vd116的值，因为
是值是进行MOV R得到的，所以两个值便为vd200和vd300的值。



4.FLAG

Flag{VD200_20.21_VD300_19.821}

- 20210624-信息化管理部-关于举办2021年工业信息安全技能大赛_03.zip

07-17
- 20210624-信息化管理部-关于举办2021年工业信息安全技能大赛
- 2021CTF工业信息安全技能大赛-工控梯形图分析1

qq_43264813的博客 1978
- 2021CTF工业信息安全技能大赛-工控梯形图分析1

小张在进行设备调试时，编写了一段模拟量转换的程序，...
- 【CTF】- 练习日志8.25-27_在某运营商的工控生产网中,存在异常数据,请...

7-22
- 题目一:ctfhub工控现场的恶意扫描 用wireshark追踪流发现 流7出现一串16进制的字符 转码直接得到flag

题目...
- 工控CTF之协议分析2——MMS_Shadow` S的博客

7-8
- 由于工控技术起步较早但是统一的协议规范制定较晚,所以许多工业设备都有自己的协议,网上资料数量视其设...

- 2020全国工业互联网安全技术技能大赛题目
含有misc, re, crypto, pwn及题目说明

10-28
- ctf工控 流量题_企业自动化运维管理员最近发现某工控设备频繁出现可疑地...

安全研究员研究工控设备发出的无线信号进行研究,发现了一些不一样的东西。Flag格式为:flag{}。 就一个这个...

7-21
- 2022工业互联网大赛-杭州-CTF题目_ctf资源-CSDN文库

第一次参加工控类的CTF,然后正好团队中有一个小伙伴电脑连不上局域网,只能从我电脑中下载下来,因此这次...

7-20
- 2021CTF工业信息安全技能大赛(常州站)-工控 APP 程序分析

qq_43264813的博客 1132

2021CTF工业信息安全技能大赛(常州站)-工控 APP 程序分析 题目内容: 在某工控人员手机中发现一个疑似远...
- 2021CTF工业信息安全技能大赛(杭州站)-简单梯形图计算

qq_43264813的博客 947

2021CTF工业信息安全技能大赛(杭州站)-PCZ 题目内容: 简单梯形图计算 解题步骤: 1.根据所给数据进行计...
- CTF竞赛题目类型_ctf网络安全大赛题库_wespten的博客

Capture The Flag(简称CTF),翻译为“夺旗比赛”,起源于1996年举办的DEF CON全球黑客大会,最早是交流安全...

7-17
- 2021年中国工业互联网安全大赛_工业互联网ctf_苦行僧(csdn)的博客-CSDN...

2021年10月14日,山东·青岛,中国工业互联网安全大赛核能行业赛道,上午9:00开始,下午5:30结束。本人与另外...

7-18
- 工控CTF (wp)

aaorong的博客 7089

这里写自定义目录标题欢迎使用Markdown编辑器新的改变功能快捷键合理的创建标题,有助于目录的生成如...
- 第七届全国工控系统信息安全攻防竞赛-梯形图

qq_43264813的博客 551

第七届全国工控系统信息安全攻防竞赛-梯形图 设备要根据当前梯形图内数值计算后对结果进行检测, 正确后...
- ...注册机2_工控互联网安全 ctf 奇怪的udp 2022 福建_summ3rf149的...

双击运行试试,发现是个MFC写的注册机,随便输入提示如右图,弹出"try Again" 窗口。 丢进IDA一通静态分析,未...

7-16
- [工控CTF]2021工业信息安全技能大赛 (江西站) -WP

3tefanie、zhou的博客 4178

西门子S7协议 查找西门子S7协议资料,发现是一个写操作,根据其报文格式,获拼接出回复报文 写demo3: ...
- 一道MMS工控协议CTF题的WriteUp

Panda - 专注于网络空间安全研究 - www.cnpanda.net 4382

0x01 赛题说明 赛题说明: 只能变电站通过 61850 规约进行监控层到间隔层的数据采集, 请分析网络数据包...
- 2021CTF工业信息安全大赛第一场题.rar

2021CTF工业信息安全大赛第一场题

09-19
- 2019工业信息安全技能大赛试题

2019工业信息安全技能大赛的CTF试题,里面存在流量题、加密、隐写、逆向、固件、工控协议、等等

07-30
- 2020工业控制安全大赛试题.zip

"中能融合杯"第六届全国工控系统信息安全攻防竞赛于9月12日上午9:00准时开赛,工控系统信息安全...

09-12
- 从CTF到工控安全.pdf

从CTF到工控安全.pdf

02-26
- 工控安全: CTF赛前小知识[转]

KEY0NE的个人博客 1469

工控比赛考察点采用 CTF 分类模型,总结分析当前工控 ICS 比赛中的关键点比赛类型考察点与 CTF 异同内...
- 2021工业信息安全技能大赛线上第二场--PLC故障分析

shutdown -s -t 675

照例先聚焦工控协议和数量较少的功能码,主要是modbus协议,功能码较少的是写单线圈指令(write single ...
- 记某工控CTF比赛一道ICMP隧道题

shutdown -s -t 2471

某塔的线上比赛平台,最后一道一堆蜜罐,听说没flag,反正没找到。然后看一下其中一道ICMP隧道的题目。...
- 2021CTF工业信息安全技能大赛(常州站)-工控图片分析

qq_43264813的博客 629

2021CTF工业信息安全技能大赛(杭州站)-工控图片分析 题目内容: 小李捕获到一份文件,请分析该文件,试...
- ctf安全竞赛入门 pdf 下载 最新发布

回答1: ctf安全竞赛是指网络安全领域的竞赛,参加者需要展示其对于各种网络安全威胁的防范和攻击技...

06-25

“相关推荐”对你有帮助?

- 非常没帮助
- 没帮助
- 一般
- 有帮助
- 非常有帮助



夜白君

码龄5年

 北京卓识网安技术...

83

6万+

2万+

11万+



原创

周排名

总排名

访问

等级

1290

351

60

108

152

积分

粉丝

获赞

评论

收藏























私信

关注

搜博主文章



热门文章

- 2021陇剑杯网络安全大赛-iOS  15348
- 2021年“绿城杯”网络安全大赛-Misc-流量分析  6296
- 2022第二届网刃杯网络安全大赛-ICS  5884
- 2022第二届网刃杯网络安全大赛-Re  4912
- 2021CTF工业信息安全技能大赛-PLC故障分析  3136

分类专栏

- 

漏洞复现

1篇
- 

HackTheBox

1篇
- 

2022第二届网刃杯网络安...

4篇
- 

2021年“莲城杯”网络安全...

13篇
- 

2021年“绿城杯”网络安全...

12篇
- 

2021陇剑杯网络安全大赛


8篇

最新评论

- 2021CTF工业信息安全技能大赛-异常的...
iscaibird: 你好，可以问一下这个ciphey怎么安装吗
- 2021CTF工业信息安全技能大赛-损坏的...
暮秋初九: 师傅你好好有原题吗
- 2021CTF工业信息安全技能大赛(常州站)...
wgf42421: 用2022没显示这条有问题。。。同样从12303开始的。
- 夜刃CTF小组招募志同道合的CTFer
_小飒: 现在是web
- 夜刃CTF小组招募志同道合的CTFer
夜白君: 什么方向

最新文章

CVE-2013-7239 Memcached未授权访问漏



夜白君

关注

 0



 4

2022第二届网刃杯网络安全大赛-Web


2023年 2篇 2022年 4篇
2021年 77篇

目录

2021CTF工业信息安全技能大赛-工控梯...

解题步骤:

- 1.使用工具打开工程图查看;
- 2.手动计算出运行过程各个点位值;
- 3.分析工程图vd120两次输入值，根...
- 4.FLAG

 夜白君

关注

 0



 4