

补充文件：

“中控杯”赛题 4 “工控信息安全攻防演练”

初赛赛题解析

一、赛题组成（总共 16 个题目，5 大类型，抽 5 道题目解读）

本次初赛共设置 16 道赛题，紧密围绕工控安全实战场景，涵盖流量分析、固件分析、Web 安全、工控组态分析及密码学五大方向。题目难度分布为：简单题 1 道、中等偏简单题 2 道、中等题 6 道、中等偏难题 4 道、难度题 3 道，对应分值分别为 100 分、150 分、200 分、300 分、400 分，旨在全面考察参赛者的工控安全综合实战能力。

以下为五大题型的核心考察内容：

（一）流量分析类题型

该题型是工控安全赛事中占比最高、最贴近实战的必考题型。比赛中将提供不同 PLC 的数据包，要求参赛者从大量工控通信数据中精准解析协议字段、提取有效流量，重点考察识别关键操作、还原工控行为的能力。

（二）固件分析类题型

本类题型为本次赛事的典型考题，主要针对施耐德 PLC 固件进行静态逆向分析。要求参赛者从固件二进制文件中定位程序逻辑、还原关键算法、挖掘隐藏数据，重点考察反汇编能力及对工控系统底层原理的理解。

（三）Web 安全类题型

该题型以一套集成了 AI 语义向量检索与重排序模型的工控知识库检索系统为背景，核心任务是找到隐藏在知识库内的 Flag。重点考察对语义搜索机制及语义黑名单绕过技术的理解。

（四）工控组态分析类题型

本题型要求参赛者读懂 PLC 工程文件，梳理完整的设备控制逻辑，精准识别程序中的异常行为，综合考察对工控编程语言及组态工具的实际掌握水平。本次比赛将提供西门子等主流厂商的组态文件供分析解题。

（五）密码学类题型

本次初赛的密码学题目不再独立设题，而是融合在其他题型中，作为解题链路的关键环节。重点考察对经典密码算法的逆向推导能力，涵盖 RSA 算法逆向与 SHA256 哈希链还原等高频方向。

二、比赛流程

参赛者访问选手登录入口，完成登录后进入平台功能界面，随后可进入赛事主界面。平台将展示答题方式、Flag 提交方法及解题报告上传流程等操作说明。

（一）赛题作答流程

比赛开始后，参赛者可在竞赛界面选择题目、下载附件，完成分析解密后将 Flag 提交至对应题目页面。

（二）实物赛题规则

本次实物赛题不全程开放，将于比赛当日中午 13:00，对当前积分榜排名前 50%的队伍开放作答权限。入围队伍可通过虚拟机远程连接实物 PLC 设备，完成实操测试与答题。

（三）解题报告提交要求

所有成功作答并获取 Flag 的题目，均须提交对应的解题报告。参赛者需在平台下载统一模板，填写完整的解题过程，并在比赛结束前上传至指定入口。未提交解题报告的题目将不予计分。

（四）评分规则与加分机制

本次初赛采用平台自动判分机制，答错不扣分，分数实时累计。同时设有一血激励规则：每道题前三名解出的队伍，分别获得该题基础分值 20%、10%、5%的额外加分，直接计入总成绩。该机制对最终排名具有显著影响，鼓励有实力的队伍积极冲刺。