

关于 2026 ISG 网络安全技能竞赛“观安杯”管理运维赛初赛的规定

一、为保障竞赛的公平、公正，确保所有解题操作可审计与回溯，本届赛事实行强制实时屏幕直播与录制。参赛者须严格遵守以下要求：

1. 直播启动与技术要求

平台自动引导：选手登录竞赛平台后，系统会自动弹出屏幕直播请求弹窗。你必须接受该请求并完成推流，无需手动访问任何外部直播页面。直播服务器由平台自动连接。

浏览器要求：竞赛平台仅支持最新稳定版 Google Chrome 浏览器。你必须使用 Chrome 访问平台，否则弹窗可能无法正常触发或推流失败。

屏幕共享范围：在浏览器弹出的共享选择窗口中，必须选择“整个屏幕”，严禁仅共享单一应用窗口或浏览器标签页。同时，严禁使用扩展屏或副显示器，将解题操作拖至副屏而主屏仅展示无关内容。所有解题活动都必须发生并完全暴露于被录制的同一屏幕内。

推流参数固化：直播推流参数（分辨率、帧率、码率等）已由平台统一固定。严禁通过浏览器开发者工具、控制台、第三方插件、脚本或任何其他手段私自修改或覆盖这些参数。

禁止虚拟化规避：禁止在虚拟机、远程桌面、云桌面或沙箱中操作解题，而只将宿主机桌面进行直播。所有解题工具必须直接运行并清晰地显示在直播画面中。

2. 直播画面内容要求

完整性：直播画面必须完整涵盖系统任务栏、系统时钟及所有解题相关窗口，不得使用图片、窗口堆叠、黑屏补丁等方式遮挡或隐藏关键操作区域。

连续性：比赛期间直播流必须保持连续，不得无故中断、暂停或录制后上传。（电脑锁屏后会中断直播，请在打开电脑后第一时间重新开启直播）

3. 竞赛操作顺序与直播强绑定

先直播后答题：必须在确认直播流成功推送、平台显示“直播在线”状态后，方可查看赛题或进行任何操作。严禁在未开启录屏的状态下预先解题。

中断即停：直播若因任何原因中断，你必须立即停止一切解题操作，直至直播恢复且平台再次确认在线。中断期间进行的任何操作和提交均视为无效。

不接受事后举证：任何没有完整直播回放的题目解答，即使 Flag 正确也一律无效。组委会不接受“未录屏但已解出”的任何解释与申诉，对应题目直接计零分。

4. 禁止干扰直播系统

严禁攻击直播服务器：禁止对竞赛直播服务器、信令服务、媒体转发节点及相关基础设施发起任何形式的网络攻击、扫描、渗透、拒绝服务攻击或恶意利用。

严禁篡改推流参数与数据流：禁止以任何方式私自修改、拦截、伪造或重定向直播推流参数及媒体数据流。

5. 赛后审核与违规判定

行为链验证：赛后裁判将根据直播回放，逐一核对 Flag 提交时间与画面操作。解题过程必须呈现信息收集、漏洞触发到获取 Flag 的完整连贯链路。若出现关键步骤跳转、凭空出现 Payload 或操作与提交时间严重不符等情况，成绩将被取消。

禁止隐蔽操作：严禁通过语音助手、第二台设备、分屏硬件等任何方式在直播画面外获取答案或帮助，而仅在画面上进行最终提交。一旦画面行为与平台日志、流量审计无法形成闭环，即判定违规。

全程可审：因自行遮挡、设备断电等个人原因导致关键操作无法被回放审查的，责任完全自负，相关题目或整场成绩将被取消。

6. 赛前测试

赛前将统一安排直播测试，请务必参加以确保设备、浏览器及屏幕共享权限正常，避免因环境问题影响参赛资格。

7. 违规处理

违反上述任一规定，裁判组有权视情节对选手或队伍处以单题计零、整场成绩取消、禁赛及通报等处罚。攻击直播基础设施的行为将直接取消参赛资格，并保留进一步追究责任的权利。

二、为维护竞赛的公平性及网络安全隔离要求，参赛者在竞赛全程中，严禁以任何形式借助外部及内部自建的人工智能系统或非授权通信渠道获取解题帮助、数据外传或内外交互。具体禁止行为包括但不限于：

1. AI 大模型与对话式 AI

禁止使用任何大语言模型、多模态模型或对话式人工智能助理（如 ChatGPT、GPT-4、Claude、Gemini、文心一言、通义千问等）进行提问、代码生成、漏洞分析、载荷构造、writeup 编写等与赛题直接或间接相关的活动。

2. AI 智能体与自动化代理（Agent）

禁止使用具有自主决策、任务规划、工具调用能力的 AI 智能体或自动化代理（如 AutoGPT、CrewAI、MetaGPT，以及各类自定义 Agent 框架），替代参赛者执行渗透测试、信息搜集、漏

洞利用、决策判断等操作。

3. AI 技能（Skill）与功能插件

禁止使用任何基于大模型的技能模块、对话插件、代码补全插件或 AI 辅助工具（包括但不限于 GitHub Copilot、Amazon CodeWhisperer、各类 ChatGPT 插件、浏览器 AI 插件、终端 AI 插件、IDE 智能插件等）直接生成或优化竞赛所使用的脚本、payload、解题思路及操作指令。

4. 第三方中转站通信与 API 代理

禁止通过任何第三方中转服务、API 代理、反向代理、隧道、云函数、Serverless 平台、Webhook 服务、内网穿透工具（如 ngrok、frp、Cloudflare Workers、消息队列、中转服务器等）将赛题内容、网络流量、环境数据或交互请求转发至外部 AI 模型或外部协助者。同时，严禁利用此类中转站绕过竞赛网络隔离策略，实现内外数据交换或远程控制。

5. 其他形式的 AI 辅助及数据外传行为

禁止以任何间接方式将竞赛相关数据发送至外部非授权系统（包括但不限于上传至在线代码运行平台、文本存储服务、即时通讯群组，或通过 API 调用方式获取 AI 生成结果）。凡借助人工智能技术代替选手独立思考与操作，或通过第三方通信手段突破竞赛环境限制的行为，均视为违规。

裁判组将在赛事过程中实时查看选手操作界面及解题情况，如发现违规现象，将直接取消本次比赛资格。