第十九届全国大学生信息安全竞赛

创新实践能力赛(总决赛)

参赛手册

为贯彻落实国家网络空间安全发展战略，加快培育兼具渗透攻击、安全防护综合素养的实战型网络安全人才，践行以赛促学、以赛促教、以赛促用核心理念，推动网络安全专业人才培养与产业需求产学研用深度融合，第十九届全国大学生信息安全竞赛-创新实践能力赛全国总决赛将如期在山东省齐鲁工业大学举行。

赛事采用 CTF 解题、综合渗透、AWD Plus 静态攻防相结合的综合竞赛模式，高度还原真实企业网络攻防场景，全方位考核参赛队伍漏洞挖掘、内网渗透、靶机加固、团队协作与实时策略研判能力。赛事由高校承办，专业网络安全企业提供竞赛靶场、流量分析等平台技术支撑，赛事面向全国高校在校学生开展选拔，旨在检验高校网络空间安全专业实践教学成效，挖掘优秀青年攻防人才，为政企、安全行业输送复合型实战后备力量。本届赛事由齐鲁工业大学（山东省科学院）承办，鹏城靶场、国家超级计算济南中心提供竞赛靶场搭建、超算算力调度等核心技术支撑，联合专业会展承接单位共同保障赛事场地、组网与后勤服务，共同为参赛选手打造安全、稳定、公平的竞赛环境。

一、比赛组织架构

比赛名称：全国大学生信息安全竞赛-创新实践能力赛。

主办单位：教育部高等学校网络空间安全专业教学指导委员会。

承办单位：齐鲁工业大学（山东省科学院）。

技术支持单位：鹏城靶场、国家超级计算济南中心、软极网

路技术（北京）有限公司、四川亿览态势科技有限公司。

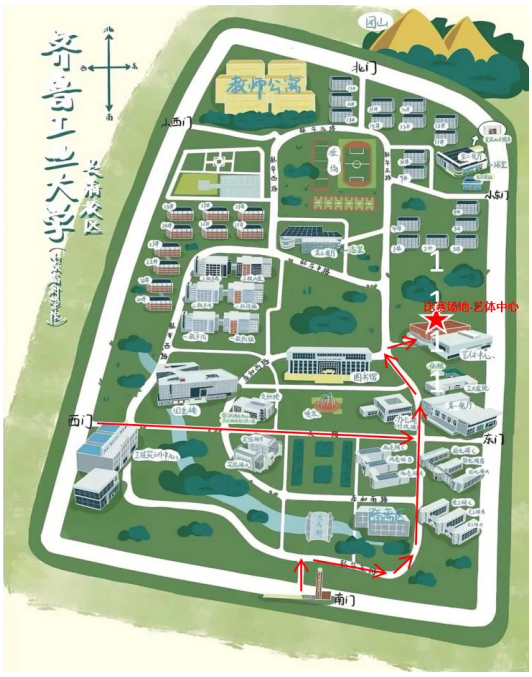
二、赛事安排

1. 比赛时间和地点

比赛时间：2026 年 8 月 29 日—2026 年 8 月 30 日。

比赛地点：齐鲁工业大学长清校区-艺体中心。导航地址：山东省济南市长清区大学路 3501 号。

公共交通路线：济南地铁 1 号线大学城（B2 口）出站——步行 515 米到达齐鲁工业大学（长清校区）南门/西门。



2. 参赛对象

经过初赛与半决赛后，排名前 80 的队伍。

3. 总决赛奖项

（1）总决赛成绩排名第 1-22 名的队伍获得全国一等奖；

（2）总决赛成绩排名第 23-46 名的队伍获得全国二等奖；

（3）总决赛成绩排名第 47 名以后的队伍获得全国三等奖；

（4）组委会根据各个分赛项比赛情况评选 10-20 名队伍授予网络安全挑战创新单项奖。

4.赛程安排

日期	时间	环节	内容
8 月 12 日 至 8 月 17 日	全天	Build 环节	1.赛题附件包下发，测试。 2.选手按照 Build 环节赛题要求完成入侵溯源分析和攻击图谱构建。 3.选手在平台提交结果截止时间为 8 月 17 日 24 时。
8 月 22 日	10:00-18:00	Build 环节成绩公布	1.公布 build 环节成绩。
8 月 28 日（星期五）	14:00-18:00	选手报到（齐鲁工业大学长清校区-艺体中心）	1.选手前往报到处进行身份验证（须携带本人有效身份证件、学生证及学校出具的在读证明）。 2.领取参赛相关资料。 3.地点：齐鲁工业大学长清校区-艺体中心。
	14:00-18:00	比赛网络环境测试（齐鲁工业大学长清校区-艺体中心）	1.选手签到后可前往比赛场地调试电脑设备，测试网络连通性，18:00 后不再开放测试环境。 2.选手测试结束后，乘坐摆渡车至酒店休息。
8 月 29 日（星期六）	7:30-8:30	选手签到（齐鲁工业大学长清校区-艺体中心）	1.选手签到，复核身份，收取手机。 2.确认比赛网络连通性。
	8:30-9:00	开幕式（齐鲁工业大	1.介绍出席领导及嘉宾。 2.全体起立奏唱中华人民共

日期	时间	环节	内容
		学长清校区-艺体中心）	和国国歌。 3.领导致辞。 4.裁判长宣读比赛规则。 5.裁判代表宣誓。 6.参赛选手代表宣誓。 7.宣布比赛开始。
	9:00-17:00	比赛环节（齐鲁工业大学长清校区-艺体中心）	1.CTF 解题赛+综合渗透赛。 2.午餐由组委会统一配送至选手工位，用餐期间比赛正常进行。
8 月 30 日（星期日）	7:30-8:00	选手签到（齐鲁工业大学长清校区-艺体中心）	1.选手签到，复核身份，收取手机。 2.确认比赛网络连通性。
	8:00-14:00	比赛环节（齐鲁工业大学长清校区-艺体中心）	1.CTF 解题赛+AWDP 攻防赛。 2.午餐由组委会统一配送至选手工位，用餐期间比赛正常进行。
	14:30-17:30	论坛（齐鲁工业大学长清校区-艺体中心大礼堂）	1. 网安学科建设与人才培养论坛。 2. 颁奖及闭幕仪式。

三、比赛方案

1.赛制说明

本次比赛共采用四种赛题模式，包括 Build 环节、CTF 竞赛、综合渗透、AWDP 竞赛模式。其中，线下比赛各环节均按比赛日期独立开放，第一天比赛题目无法在第二天继续解答。

（1）Build 环节

环节名称：基于多源日志的攻击溯源工程。

比赛时间：8 月 12 日 9:00-8 月 17 日 24:00。

比赛形式：线上参赛。

核心规则：参赛队伍需分析组委会提供的企业多源日志、网络流量及 Windows 事件记录，识别攻击证据，还原攻击时间线和攻击路径，并按规定格式提交证据集、攻击图及 IOC。

考核重点：多源数据处理与关联分析、攻击证据发现、攻击阶段判定、复杂攻击路径还原、攻击图谱构建及工程实现能力。

积分规则：参赛队伍须在规定时间内将 Build 成果提交至平台，组委会将对所有提交内容进行审核评分。每队最多提交 3 次，最终成绩取最高分。

分数规划；格式合规 10 分+证据发现 25 分+攻击阶段分类 10 分+时间线还原 15 分+拓扑节点 10 分+拓扑边关系 20 分+IOC 提取 10 分。

最终得分：战队得分/规划分值*100 分。

表 1 Build 环节考核内容

题目类型	类型描述
多源日志分析与攻击溯源	基于模拟企业环境的网络流量、服务器日志、Windows 事件日志、应用审计日志和安全告警等多源数据，考察参赛队伍的数据处理、关联分析、攻击证据识别、攻击路径还原及攻击图构建能力，参赛成果按照统一格式提交并由平台自动评分。

（2）CTF 竞赛

比赛时间：8 月 29 日 9:00-17:00，共计 8 小时；

8 月 30 日 8:00-14:00，共计 6 小时。

CTF 比赛第一天题目无法在第二天进行解答。参赛队伍通过与在线环境交互或离线分析文件，解决区块链技术、信息隐藏、国产密码、工控技术等方向的安全技术挑战，获取题目预设 flag。比赛强调单点技术深度、代码编写与独立漏洞分析能力，侧重选手单项技术功底。

参赛队伍独立完成各类安全题目，互不干扰，不存在互相攻击、防守对抗环节，得分仅依靠自主解题获取对应 Flag 分值，无靶机防护、对抗博弈相关操作。参赛队伍拥有独立操作环境，各队伍任务环境完全隔离，无交互对抗逻辑。

积分规则：采用动态积分制（每题得分除去题目预设分外，对解出题目的队伍根据结题时间获得奖励分，按总分由高到低排名，同分则以提交时间为准，用时短者优先。

最终得分=（当前队伍分数/最高队伍分数）*100 分。

表 2 CTF 赛制考核内容

题目类型	类型描述
网络安全	该类型包括 Web 应用架构、二进制程序机制、密码算法原理、杂项数据特征及逆向工程目标的安全特性与潜在风险；能够通过 SQL 注入、缓冲区溢出、算法缺陷利用、反编译分析等方式构建攻击路径；并结合代码审计、动态调试、密码分析、数据取证、逆向工程等技术，完成 Web 渗透、权限提升、密码破解、信息提取与程序逻辑还原。
区块链技术	该类型包括链上运行机制、智能合约安全、DeFi 业务逻辑、链上数据分析等内容，重点考察参赛选手对区块结构、交易流程、账户模型、Gas 机制、合约调用关系和资产流转路径的理解能力。题目可结合合约审计、漏洞分析、交易追踪、权限校验、签名验证等场景，评价选手发现问题、还原攻击过程、构造验证思路及提出修复建议的综合能力。
工控安全	该类型包括工业控制系统架构、现场设备通信、工业协议分析、PLC 逻辑及生产网络边界防护等内容设置赛题，重点考察参赛选手对 OT 环境中设备关系、业务流程和通信特征的理解能力。
信息隐藏	该类型包括围绕图像、音频、视频、文档、压缩包及网络流量等载体中的隐蔽信息提取，重点考察参赛选手对文件结构、编码方式、元数据特征和隐写痕迹的分析能力。

（3）综合渗透竞赛

比赛时间：8 月 29 日 9:00-17:00，共计 8 个小时（并行）。

核心规则：本次综合渗透竞赛采用全流程实战逐层渗透考核模式，定型为线下实操演练竞赛。竞赛搭建内网业务环境，划分互联网区、DMZ 隔离区、内网业务区，还原多层边界防火墙、路由访问控制等真实网络防护架构，部署多类业务靶机。

竞赛实行独立环境机制，每支参赛队伍分配一套专属靶场环境，队伍之间环境相互隔离、互不干扰。

考核重点：参赛队伍需遵循网络边界访问逻辑，逐层突破区域防护壁垒，综合运用信息收集、漏洞利用、权限提升、内网横向移动等攻防技术，逐级获取各节点靶机权限，搜寻隐藏 Flag 完成全链路渗透通关。

积分规则：不同 Flag 设置差异化分值，队伍总分由成功获取的 Flag 分值累加得到，比赛中队伍成功获取所有 Flag 对应的分值，最后统计所获取 Flag 总数，获取相应的分值，如获取的 Flag 总数相同，则通过提交 Flag 的时间对比，用时最短者获取相应的激励分：

最终得分:（当前队伍分数/最高队伍分数）*100 分。

表 3 综合渗透赛制考核内容

题目类型	类型描述
外网初始突破	选手从互联网区开展信息探测、漏洞利用，突破外层边界防护，获得初始立足点与 Flag，实现进入 DMZ 区。
内网纵深横向渗透	依托外网权限穿透边界，获取内网访问凭证、通道资源，开展权限提升、凭证窃取、内网横向移动，多节点持续拓展权限。
区块链专项渗透	基于区块链智能合约仿真环境开展渗透，覆盖重入攻击、未授权访问、私钥泄露等典型区块链安全风险。选手通过合约漏洞利用、密钥窃取等方式完成攻击目标，获取专项 Flag，考核区块链应用攻防能力。

（4）AWD Plus 模式（静态攻防解题加固赛）

比赛时间：8 月 30 日 8:00-14:00，共计 6 小时。

核心规则：将企业或院校等真实网络结构抽象为竞赛平台模拟环境，参赛队需同时扮演攻击方与防守方。

考核重点：实时挖掘对手环境漏洞并提交 flag 获取攻击分；修复自身环境漏洞以获得防御分。

积分规则：采用周期动态积分制，每个周期的动态积分随攻防队伍数量动态调整，对应分值随战队成功攻克或完成防御数量增加而递减。攻击成功与防御成功分别累计周期动态积分。最终按总分由高到低排名，同分则以提交时间为准，用时短者优先。

最终得分=（当前队伍分数/最高队伍分数）*100 分。

表 4 AWDP 赛制考核内容

题目类型	类型描述
Web 应用服务	考察选手对 Web 应用源码、框架逻辑和业务流程的安全分析能力，能够从 PHP、Java、Python、Golang 等常见开发语言及其运行环境中识别潜在风险，发现认证授权、输入校验、文件处理、反序列化等方面的安全问题。同时，要求选手具备对常见 Web 防护机制的理解与绕过分析能力，能够结合漏洞成因、代码逻辑和业务场景完成利用验证，并提出相应的修复与加固方案。
二进制应用服务	考查选手对 Linux 及嵌入式环境下二进制程序的逆向分析、漏洞定位和调试验证能力，能够运用静态分析与动态调试方法，识别栈溢出、堆溢出、UAF、格式化字符串等典型内存安全问题。选手需结合程序控制流、汇编指令、运行环境及保

题目类型	类型描述
	护机制，完成漏洞利用思路构造、指令级修补或 ROP 链分析，并进一步给出程序修复和安全加固建议。

四、比赛规则

1.计分规则

（1）团队计分

每队由不多于 4 名参赛选手+不多于 1 名指导教师组成，成绩按照团队选手成绩计算。

（2）总分加权算法

总成绩计算分值为 100 分，具体分数占比如下：

Build 环节成绩占总比分权重 5% + CTF 解题赛成绩占总比分权重 30% + 综合渗透赛成绩占总比分权重 30% + AWDP 攻防赛成绩占总比分权重 35%。

（3）初赛及分区赛成绩不计入决赛排名。

2.比赛期间注意事项

（1）每支参赛队的选手自备合规笔记本电脑 1 台、电源适配器、网络转接器等必须的设备,现场提供六类网络跳线；

（2）为保证比赛公平及赛场用电安全，每个参赛队员限带一台笔记本电脑，额定功率不超过 260W，以电源适配器标称额定功率为准；

（3）禁止携带路由器、随身 WiFi、手机热点、无线鼠标/键盘、无线耳机、存储设备、边缘 AI 计算设备等违规物品，所有设备须通过赛前安检；

（4）选手需关闭浏览器的广告拦截插件和网络代理，保证平台的正常访问；

（5）推荐选手使用 Chrome 或 Firefox 浏览器进行答题。若选手使用其他浏览器需自己负责兼容性问题；

（6）在网络配置确认阶段和正式比赛期间，选手须使用同一台终端设备，防止因临时调换设备导致网络故障，影响答题；

（7）比赛期间赛场将启用信号屏蔽设备，无线鼠标、无线键盘等无线设备可能无法使用，请选手自备有线设备。

3.赛场规则

（1）参赛队伍需提前 30 分钟到达比赛地点，凭有效证件核验身份后参赛。线下比赛前，所有参赛选手需将手机上交至组委会统一保管，赛后统一归还。比赛现场将为每支参赛队伍提供四个标准网络接口，参赛选手需自行携带笔记本电脑及兼容本人电脑的网络转接头。

（2）选手需自备个人参赛工具：笔记本电脑、鼠标、鼠标垫、键盘、网口转接器，自己熟悉的参赛环境和常用软件、工具、脚本等。用于登录比赛系统的 VPN、用户名和密码将在比赛签到时统一发放。

（3）比赛过程中，参赛选手通过 VPN 的方式访问竞赛平台获取题目信息，赛题环境需要拨通 VPN 后进行访问（赛前提供选手操作手册）。每位参赛选手分配 1 个 VPN 账号，每个账号仅支持 1 台终端设备保持在线，不能在多个终端同时登录。

（4）选手进入比赛环境后，系统将展示比赛状态、起止时间等信息，待比赛开始后可进入详情页进行比赛。比赛攻击时段可提交 Flag，防守时段可上传防御包。更多信息请查询现场发放的操作手册。

4.反作弊规则

（1）禁止任何对比赛相关平台的暴力破解和攻击；

（2）禁止 DDoS、ARP 等干扰比赛正常进行的攻击；

（3）禁止任何针对参赛对手的网络攻击行为；

（4）比赛过程中禁止参赛队伍之间分享任何解题思路及 FLAG；

（5）违规处罚采用轻度、中度、重度三级处罚体系：对场外交流、私连外网等轻度违规行为给予警告扣分；对恶意攻击非目标平台、篡改赛题环境等中度违规行为扣除该队 50%总分；对作弊传题、恶意流量压测等重度违规行为取消参赛成绩并通报所属高校，全程记录留痕、可追溯取证。

五、违规处理、举报申诉与仲裁规则

为维护赛事公平公正，保障赛事顺利开展，现将违规处理、举报申诉与仲裁相关规定明确如下：

1.违规处理

出现以下情形，裁判组将立即取消参赛资格与比赛成绩，情节严重者将通报至参赛队伍所在高校。

（1）参赛报名信息作弊或造假，包括但不限于编造成员身份、冒用他人身份参赛等；

（2）在参赛过程中出现违反相关法律、法规的行为；

（3）在参赛过程中经发现或被举报并认定存在违反赛事要求的行为，如抄袭他人成果、使用违规工具等。

2.举报与申诉

（1）举报流程：参赛选手若发现其他队伍违规，可进行实名举报，举报时须提交清晰、完整的佐证材料（如截图、视频、文字记录等），由大赛组委会秘书处负责受理。匿名举报或无有效佐证材料的举报将不予处理；

（2）申诉流程：对成绩或评判存在异议的参赛选手，需在比赛结束后 2 天内，向大赛组委会秘书处提交书面申诉报告。报告内容应清晰地阐述申诉内容，详细说明争议点，并附参赛队伍指导教师及全体队员签名，未按要求提交的申诉将不予受理。

3.仲裁机制

大赛组委会秘书处负责接收举报和申诉材料，并提交技术委员会进行仲裁。技术委员会依据赛事规则、相关证据，对举报和

申诉事项进行审议，其做出的仲裁结果为最终决定。举报和申诉的受理截止时间为比赛结束后 2 天内，逾期将不再受理。

六、联络信息

总决赛期间，具体活动时间以官网公布为准。

赛事相关联系人：

（Build 环节）电话：郝老师 18673175134

（线下赛环节）电话：郑老师 17377782635

（酒店交通事务）电话：张老师 17668777939

参赛选手 QQ 群：1094058805

指导教师 QQ 群：1092498027

大赛秘书处邮箱：1531734383@qq.com

入住及交通推荐：

出行路线及酒店推荐.docx

七、其他

赛事举行期间，参赛队伍及队员的交通、食宿费用需自理，请各位参赛人员自行安排好出行事宜，合理规划，确保按时参赛。如有任何疑问，请及时与赛事联系人沟通。

本决赛规程的最终解释权归第十九届全国大学生信息安全竞赛——创新实践能力赛组委会所有。

第十九届全国大学生信息安全竞赛

-创新实践能力赛竞赛组委会

（齐鲁工业大学网络空间安全学院代章）

2026 年 8 月 11 日