第十八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，加速培养具有实战能力的攻防创新人才，践行以赛促学、以赛促教、以赛促用理念，助力网络空间安全人才培育及产学研用深度融合，由郑州大学承办，永信至诚科技集团股份有限公司提供平台技术支撑，奇安信科技集团股份有限公司、北京天融信教育科技有限公司、绿盟科技集团股份有限公司、郑州云智信安安全技术有限公司赞助的第十八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于2025年7月在河南郑州举行。

一、赛事安排

1.比赛时间和地点

比赛时间：2025年7月19日至7月20日

比赛地点：中国网络安全科技馆四楼赛博厅（河南省郑州市高新区河阳路186号）

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. 赛事日程安排

表 1 日程安排表

日期	时间	环节	内容
7 月 4 日 至 7 月 5 日	4 日 10:00 -5 日 18:00	Build 环节 第一次提交 （线上）	1. 按照 Build 环节赛题要求完成知识库构建与安全检测项创新设计 2. 7 月 8 日公布第一次 Build 成绩
7 月 11 日 至 7 月 12 日	11 日 10:00 -12 日 18:00	Build 环节 第二次提交 （线上）	1. 按照 Build 环节赛题要求完成知识库构建与安全检测项创新设计 2. 7 月 16 日公布第二次 Build 成绩
7 月 18 日 （星期五）	14:00-18:00	选手报到 （入住酒店）	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：郑州高新假日酒店一层大堂（中国网络安全科技馆北 20 米）
	17:00-19:00	比赛网络环境测试（中国网络安全科技馆四楼赛博厅）	1. 选手前往比赛场地调试电脑设备及测试网络连通性
		实体车参观（网络安全科技馆一楼正门大厅）	1. 选手可参观车联网赛题实体车辆 2. 车联网基础知识内容分享
7 月 19 日 （星期六）	7:30-8:30	选手签到（中国网络安全科技馆四楼赛博厅）	1. 选手签到，复核身份，收取手机 2. 选手确认比赛网络连通性
	8:30-9:00	开幕式（中国网络安全科技馆四楼赛博厅）	1.介绍出席开幕式领导及嘉宾 2.全体起立，奏唱中华人民共和国国歌 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
	9:00-15:00	比赛环节（中国网络安全科技馆四楼赛博厅）	1. CTF 解题赛+综合渗透赛 2. 午餐由组委会提供盒饭，用餐期间比赛正常进行
7 月 20 日 （星期日）	7:30-8:00	选手签到（中国网络安全科技馆四楼赛博厅）	1.选手签到，复核身份，收取手机 2.选手确认比赛网络连通性
	8:00-14:00	比赛环节（中国网络安全科技馆四楼赛博厅）	1. CTF 解题赛+AWDP 攻防赛 2. 午餐由组委会提供盒饭，用餐期间比赛正常进行
	14:30-18:00	论坛、闭幕式及颁奖（中国网络安全科技馆四楼赛博厅）	1. 网安人才培养论坛 2. 冠军解题思路分享 3. 颁奖及闭幕仪式
	18:00-19:00	参观中国网络安全科技馆	1. 专业讲解，分组参观中国网络安全科技馆（一、二、三层）
	19:00-20:00	晚餐（中国网络安全科技馆四楼赛博厅）	1. 大赛参赛选手交流活动

二、比赛方案

1.赛制说明

（1）半开放命题攻防模式

决赛采用半开放命题攻防模式：由Build（知识库构建与安全检测项创新设计）与Break&Fix（攻击防御综合对抗）两大环节构成。

（2）分值占比

Build环节占总分5%，Break&Fix环节占总分95%。

（3）Build环节

比赛时间：7月4日-5日、7月11日-12日

比赛形式：线上参赛

比赛内容：具体细则参照官网Build环节《知识库构建与安全检测项创新设计参赛指南》。

（4）Break&Fix环节

比赛时间：7月19日-7月20日

比赛形式：线下参赛

比赛内容：CTF解题赛+综合渗透赛+AWDP攻防赛的混合赛制

2.考核形式及内容

（1）Build环节

比赛时间：7 月 4 日 10:00-5 日 18:00

7 月 11 日 10:00-12 日 18:00

核心规则：根据操作指南提交知识库及安全检测项设计。

考核重点：数据收集的全面性与有效性、数据清洗的规范性与精准度、知识库体系建设的逻辑性与完整性、安全检测原理及应用场景的理解深度。

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。最终成绩以参赛队伍两次提交中的最高分为准。

最终得分=（知识库构建分数/最高知识库构建分数）*80 分+（安全检测项设计分数/最高安全检测项设计分数）*20 分

表 2 Build 环节考核内容

任务名称	任务描述
知识库构建	选手需围绕设定的网络硬件设备安全、大模型安全，构建结构化的安全知识库；选手应根据方向提示，梳理相关安全信息，进行数据清洗与归类整合，最终提交具备组织性、查询性与实用性的知识库。
安全检测项设计	选手需基于主办方提供的企业内网环境下 AI 模型部署的基础检测项，深入分析内网安全需求，创新性设计出新增安全检测项；进一步完善企业内网整体安全检测体系，最终提交包含原有基础检测项以及设计的新增安全检测项的检查项测试集。

（2）CTF 解题赛

比赛时间：7 月 19 日 9:00-15:00，共计 6 小时。

7 月 20 日 8:00-14:00，共计 6 小时。

核心规则：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，解决网络安全、可信计算、车联网安全、AI 模型安全等方向的安全技术挑战，获取题目预设 flag。

考核重点：网络安全、可信计算、车联网安全、AI 模型安全知识。

积分规则：采用动态积分制（每题分值随解出队伍数增加而递减），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 3 CTF 赛制考核内容

题目类型	类型描述
网络安全	要求选手理解 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。

可信计算	考察选手应用可信密码技术支持现实环境信任的实践能力，并可体验自主可信计算下可信密码的组件化使用方式。
车联网安全	考察选手对车端系统与通信协议的安全分析能力；理解车端系统（如IVI，TBOX等）和通信接口（如ADB、Telnet、OTA、CAN、UDS等）的安全特性与潜在风险；能够通过接口暴露、服务配置错误、协议缺陷等方式实现攻击入口；并结合渗透测试、逆向分析与报文分析等技术，完成漏洞利用、权限获取与服务安全加固。
AI模型安全	考察选手对AI模型投毒、权重窃取、样本攻击与模型反演的构造评估能力；理解数据集处理、权重存储、样本输入及模型接口的安全风险；能通过恶意注入、接口暴露、样本漏洞、反演路径实现攻击入口；并结合数据污染、权重分析、样本对抗、反演算法等技术，完成漏洞利用、模型衰减、权重盗取与隐私还原。

（3）综合渗透赛

比赛时间：7月19日9:00-15:00，共计6小时。

核心规则：参赛选手扮演渗透测试团队，按参赛任务要求对指定网络环境实施渗透，目标为获取关键资产；同时需依据检测项测试集，对指定场景的配置进行安全核查。

考核重点：考察信息搜集、外网打点、横向移动、特权提升、域渗透、权限维持等渗透技术，以及系统环境配置问题的检测能力。

积分规则：采用动态积分制（每题分值随解出队伍数增加而递减），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 综合渗透赛赛制考核内容

题目类型	类型描述
信息搜集	通过各种方法收集目标系统的详细信息，为后续渗透提供基础。
外网打点	利用目标网络外部入口的漏洞进行初步渗透，获得系统访问权限，建立立足点。
横向移动	在已经获取访问权限的系统内部，通过网络进行横向扩展，访问更多的主机和资源。
特权提升	在已控制的系统上，通过漏洞或配置错误提升权限，从普通用户变为管理员。
域渗透	针对目标网络的域环境，通过一系列技术手段获取域内的高级权限。
权限维持	在成功渗透目标网络后，使用后门、持久性脚本等手段维持长期访问权限。
AI 模型的部署安全	在众多本地化部署的 AI 模型运行框架中，主要包含访问控制、模型窃取、运行时漏洞、对抗性攻击、资源滥用和数据隐私等相关的安全问题。

（4）AWDP 攻防赛

比赛时间：7 月 20 日 8:00-14:00，共 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：采用动态积分制，每题分值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动态积分，违规行为将导致队伍扣分。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 5 AWDP 赛制考核内容

题目类型	类型描述
Web 应用服务	考察选手从源代码中精准识别和分析安全漏洞的能力；理解 PHP、JAVA、Python、Golang 等主流编程语言的安全特性与潜在风险；同时能够识别并绕过各类 Web 防护系统，通过构造复杂攻击链实现漏洞利用与防护突破；进而结合代码逻辑、业务场景和防护需求，完成漏洞修补与安全加固。
二进制应用服务	考察选手对 Linux 与嵌入式设备中二进制文件的深入分析能力；掌握静态与动态调试技术，能够识别并利用栈溢出、堆溢出、UAF、格式化字符串等典型漏洞；结合汇编指令 patch、ROP 构造等手段实现漏洞利用并获得目标系统权限；同时能够结合程序逻辑、系统环境与安全需求，完成漏洞修复与防护加固。

3. 总成绩计分规则

（1）团队计分

每队最多 4 人，成绩按照团队成绩计算。

（2）总分加权算法

总成绩=Build 环节成绩***5%**+（CTF 解题赛成绩*20% + 综合渗透赛成绩*40% + AWDP 攻防赛成绩*40%）***95%。**

（3）初赛及分区赛成绩不计入决赛排名

4.比赛期间注意事项

（1）选手需自备连接网络所需要的设备，如 USB 转 RJ45 转换器等工具；

（2）为保证比赛公平及赛场用电安全，每名选手只允许携带一台电脑，且功率不超过 150W，不允许携带超过指定功率的设备，例如：功率超标的专业工作站、搭载神经网络芯片的 AI 一体机等；

（3）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；

（4）选手需使用 Chrome 或 Firefox 浏览器进行答题，若使用其他浏览器请开启极速模式或兼容模式；

（5）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。

三、比赛要求

1. 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；比赛期间，赛场将启用信号屏蔽仪，无线鼠标、无线键盘等设备或将无法使用，参赛选手需根据自身需求自备有线设备；

2.线下比赛期间，所有参赛选手需要对比赛所使用的电脑进行屏幕录制。参赛选手可根据不同机型及操作系统自行选择录屏软件（推荐使用 EVCapture 录屏软件、OBS 录屏软件、Mac 自带录屏软件 QuickTime 等），参赛选手需在赛前进行下载安装及调试，正式比赛时不再提供下载安装及调试时间。使用部分录屏软件时，录制时长过久会造成视频数据无法及时写入硬盘，使得内存中堆积大量数据，录屏软件申请不到新的内存而停止，从而导致录屏失败。因此，请参赛选手根据不同软件所需，每 2 小时或 3 小时保存一次录屏文件，随后马上开启新的一次录屏。除手动保存录屏文件外，比赛期间屏幕录制不能中断；

3.参赛选手不得私自搭建网络代理将综合环境进行转发；

4.比赛过程中禁止攻击平台或干扰其他选手正常比赛，禁止对题目场景进行破坏；

5.所有参赛选手（同一队伍的队员除外）禁止使用即时通信软件等渠道与其他人员进行赛题内容沟通交流；禁止不同队伍之间合作或共享 flag、hint 等任何比赛相关信息；禁止使用在线、连接网络的 AI 工具，可以使用本地化 AI 模型；

6. 比赛平台采用严格的反作弊监控机制，对于过程中发现作弊、串题或对比赛平台恶意攻击的行为，将采取禁赛、直接取消比赛成绩等处罚措施，情节严重者将由组委会通报参赛队伍所在高校；

7. 参赛选手如有问题，可向工作人员询问；

8. 比赛过程中若发现意外情况，须听从工作人员管理和指挥。

四、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。

五、联络信息

总决赛期间，具体活动时间以官网公布为准。

联系人：

曹老师 郑州大学（技术问题）电话：13733851010

王老师 郑州大学（其他事务）电话：18838980800

苗老师 永信至诚（平台支撑）电话：18503890126

王老师 永信至诚（平台支持）电话：15011466199

参赛选手 QQ 群：1046816089

指导教师 QQ 群：458106365

大赛秘书处邮箱：ciscn_zzu_2025@163.com

附件：交通和住宿推荐

交通和住宿推荐.docx

六、其他

会议期间，食宿费用需自理，请各位参赛人员自行安排好食宿事宜，合理规划出行，确保按时参赛。如有任何疑问，请及时与会议联系人沟通。

本决赛规程的最终解释权归第十八届全国大学生信息安全竞赛——创新实践能力赛组委会所有。

第十八届全国大学生信息安全竞赛

创新实践能力赛竞赛组委会

（郑州大学网络空间安全学院，代章）

2025 年 7 月