

全国大学生信息安全竞赛组织委员会

第十六届全国大学生信息安全竞赛 创新实践能力赛决赛参赛手册

为积极响应国家网络空间安全人才需求，加快攻防兼备创新人才培养步伐，实现以赛促学、以赛促教、以赛促用，推动网络空间安全人才培养和产学研用生态体系建设，由国防科技大学、中国科学技术大学联合承办，南京赛宁信息技术有限公司提供平台支持的第十六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 2023 年 7 月在安徽合肥举行。

一、赛事安排

(1) 比赛时间和地点

比赛时间：2023 年 7 月 24 日至 7 月 26 日

比赛地点：中国书法大厦（安徽省合肥市高新区科学大道 69 号）

(2) 参赛对象

全国 8 个分区赛一等奖获奖队伍。

(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。

全国大学生信息安全竞赛组织委员会

(4) 赛事日程安排

表 1 日程安排表

日期	时间	环节	内容
7月3日至 7月19日	全天	Build 环节	按照 Build 环节赛题要求完成创新应用开发
7月24日	14:00 - 18:00	报到	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
	17:00 - 19:00	比赛网络环境测试	选手前往比赛场地调试电脑设备及测试网络连通性
7月25日	8:00 - 8:30	选手签到及确认账号	1. 选手签到, 复核身份, 收取手机 2. 发放参赛须知 3. 选手登录账号确认比赛网络连通性及账号信息
	8:30 - 9:00	开幕式	1. 介绍出席开幕式领导及嘉宾 2. 全体起立, 升国旗, 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 - 17:00	比赛环节	1. CTF 解题赛+AWD 网络攻防赛 2. 午餐由组委会提供盒饭, 用餐期间比赛正常进行
7月26日	8:00 - 14:00	比赛环节	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
	14:30 - 17:00	论坛及颁奖	1. 网安人才培养论坛 2. 冠军解题思路分享 3. 颁奖仪式
	17:30-19:00	晚宴	

全国大学生信息安全竞赛组织委员会

二、比赛方案

(1) 赛制说明

1. 决赛采用半开放命题形式的攻防竞赛模式，由 Build（创新安全应用开发）、Break&Fix（攻击、防御综合对抗）两个环节组成，其中 Build 环节占比总分 15%，Break&Fix 环节占比总分 85%；

2. Build 环节比赛时间为 7 月 3 日至 7 月 19 日，比赛形式为线上参赛，比赛内容为网络空间测绘创新应用开发，具体比赛细则参照官网 Build 环节创新应用设计指南；

3. Break&Fix 环节比赛时间为 7 月 25 日至 7 月 26 日，比赛形式为 CTF 解题赛+AWD 网络攻防赛+综合渗透赛的混合赛制，从多个方面综合考察个人的安全综合技术能力及团队协作解决实际网络安全问题的能力。

4. CTF 解题赛中，参赛队伍通过与在线环境交互或文件离线分析，解决网络安全技术挑战并获取题目预设的 Flag 值从而获取相应分值。CTF 解题赛比赛时间为 7 月 25 日至 7 月 26 日，比赛第一天题目无法在第二天进行解答。CTF 模式题目涵盖可信计算、工控安全、量子安全、人工智能安全等，详情见表 2。

表 2 CTF 赛制考核内容

题目类型	类型描述
人工智能安全	主要包括针对人工智能系统和应用程序的多样攻击技术，如对抗性输入、数据中毒攻击及模型窃取技术。常见考察点分为实现 AI 模型自动化操作和利用基于神经网络欺骗的方式对目标 AI 模型进行欺骗。
工控安全	主要包括流量分析、无线电分析、组态分析、梯形图等方

全国大学生信息安全竞赛组织委员会

	向，并且还会涉及工控程序分析、固件分析和无线电频谱、波形、编解码分析等。
可信计算	主要包括模拟真实系统的实际场景、自动控制逻辑和人员业务操作流程，及在这一环节下的网络攻击行为（来自仿冒者、入侵者、篡改者、拦截者和潜伏者等攻击角色），要求解题者通过完善系统安全机制来抵御不同角色发起的攻击行为。
量子安全	量子计算机攻击技术：掌握量子计算机攻击的原理和方法，如量子搜索算法、Shor 算法等。 量子安全加密：熟悉常见的量子安全加密算法，包括基于量子密钥的加密算法和基于量子态的加密算法。

5. AWD 网络攻防赛采取经典的 attack 和 defence 模式，题目类型覆盖 WEB 及 PWN，重点考察参赛团队漏洞挖掘、漏洞利用、漏洞修补、流量分析、团队协作等多方面的能力。初始时刻所有参赛队伍拥有相同系统环境 GameBox，每台 GameBox 中的 Flag 采用动态更新机制。在每个回合中，参赛战队维护多台服务器，服务器中存在多个漏洞，利用漏洞攻击其他队伍可以得分，自身服务器存在的漏洞被其他队伍攻击则失分，因修补漏洞导致的自身服务器宕机将扣分。比赛时间为 7 月 25 日共计 8 个小时。

6. 综合渗透赛深度模拟真实网络环境，参赛队伍模拟攻击者，通过信息收集、拓扑测绘、外网渗透、资产数据发现以及内网横向移动等多种方式，最终完成仿真环境的渗透过程。综合渗透赛中，平台为每个参赛战队提供独立的赛题系统环境；环境为多层网络，包含跳板机和非跳板机，需要通过跳板机才能进入到下一层网络继续答题。比赛考核的知识点见表 3。

表 3 综合渗透赛考核内容

题目类型	题目描述
外网突破	信息搜集

全国大学生信息安全竞赛组织委员会

	WEB 漏洞扫描 WEB 漏洞利用 数据库漏洞利用 中间件漏洞利用
内网渗透	内网信息搜集 操作系统漏洞利用 Metasploit 使用 凭据提取 横向移动 隧道技术 持久化技术

7. 比赛期间，CTF 解题赛和 AWD 网络攻防赛的赛题分阶段放出，综合渗透赛赛题一次性放出。

(2) 单项计分规则

1. Build 环节具体评分规则参照官网 Build 环节创新应用设计指南；

2. CTF 解题赛采用动态积分的方式进行评分，获取赛题中的 Flag 并提交竞赛平台而得分。题目分值随着解题队伍数量的增加将随之减少，且所有解出此题的队伍所持有的分数都会动态减少。每道赛题前三名队伍可以额外获得当前题目分值 5%、3%、1%的奖励分值。CTF 解题赛最终分数计算公式如下：

最终得分 = (当前队伍分数 / 最高队伍分数) * 100 分

3. AWD 网络攻防赛采用回合制零和游戏机制进行评分，攻击成功一个 Gamebox 并提交获取的动态 flag 获得 50 分，被获取 flag 的参赛战队该题目将丢失 50 分；各参赛战队在进行漏洞修补的过程中必须保证己方赛题的正常工作并通过平台每回合的

全国大学生信息安全竞赛组织委员会

功能 Check，如赛题宕机或无法通过功能 Check，则宕机参赛战队失去 50 分；每回合内，每道赛题 Check 异常与宕机，被拿 flag 可以同时累计失分。AWD 攻防赛最终分数计算公式如下：

最终得分=（当前队伍分数/最高队伍分数）*100 分

4. AWD 网络攻防赛模式中，各参赛战队在比赛开始时须对所有赛题进行备份，若因自身原因导致赛题环境永久损坏或丢失，无法恢复，主办方不提供重置服务。如若参赛战队要求重置赛题环境，每道赛题每重置一次扣除 1000 分（在比赛结束后统一扣除）。

5. 综合渗透赛采用动态积分机制进行评分，参赛队伍模拟攻击者进行场景接入、攻击、渗透等操作，拿到赛题的 Flag 即可得分。题目分值随着解题队伍数量的增加将随之减少，且所有解出此题的队伍所持有的分数都会动态减少。每道赛题前三名队伍可以额外获得当前题目分值 5%、3%、1%的奖励分值。综合渗透赛最终分数计算公式如下：

最终得分=（当前队伍分数/最高队伍分数）*100 分

（3）总成绩计分规则

1. 选手以组队形式（最多 4 人）参赛，成绩按照团队成绩计算。

2. 决赛采用加权算法，Build 环节占比总分 15%，Break&Fix 环节占比 85%。在 Break&Fix 环节中，CTF 解题赛占比 30%，AWD 网络攻防赛占比 40%，综合渗透赛占比 30%，其具体计算方法如

全国大学生信息安全竞赛组织委员会

下：

总成绩=Build 环节成绩*15%+（CTF 解题赛成绩*30%+AWD 网络攻防赛成绩*40%+综合渗透赛成绩*30%）*85%

3. 初赛成绩及各分区赛成绩不纳入决赛排名的参考依据。

（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. 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；

3. 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答题；

4. 在网络配置确认阶段和正式比赛期间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）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）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；

（3）所有参赛队员（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；

全国大学生信息安全竞赛组织委员会

(4) 参赛选手不得私自搭建网络代理将靶场环境进行转发；

(5) 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；

(6) 参赛选手如有问题，可向工作人员询问；

(7) 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

以下情况将视为违规，裁判组将立即取消其参赛资格和比赛成绩，情节严重者将通报参赛队伍所在高校：

(1) 参赛报名信息作弊或造假；

(2) 在参赛过程中出现违反相关法律、法规的行为；

(3) 在参赛过程中发现或者被举报认定存在违反“比赛要求”的行为。

五、举报、申诉与仲裁

(1) 参赛选手可对其他队伍的违规行为进行举报，举报须实名且提交佐证材料，由大赛组委会秘书处负责受理；

(2) 参赛选手对成绩或者评判有异议的，可向大赛组委会秘书处提出书面申诉报告，申诉报告应明确申诉内容且附有参赛队伍指导教师及全体队员签名，否则申诉将不予受理；

(3) 大赛组委会秘书处负责受理举报和申诉，并报技术委

全国大学生信息安全竞赛组织委员会

员会仲裁，技术委员会作出的仲裁结果为最终决定。受理截止时间为比赛当天 17:30。17:30 前选手需签署成绩确认单，17:30 后未签字确认者视为自动确认成绩。

六、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：李老师（国防科技大学） 电话：18110991801

吴老师（中国科学技术大学） 电话：13855170994

竞赛 QQ 群：835661393

教师 QQ 群：807214878

七、其他

本总决赛规程的最终解释权归第十六届全国大学生信息安全竞赛—创新实践能力赛组委会所有。

第十六届全国大学生信息安全竞赛
——创新实践能力赛竞赛组委会
(国防科技大学电子对抗学院代章)

2023 年 7 月 12 日