教育部高等学校网络空间安全专业教学指导委员会

第十二届全国大学生信息安全竞赛—创新实践能力赛参赛规程与指南

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，从而推动网络空间安全人才培养和产学研用的生态体系，由教育部高等学校网络空间安全专业教学指导委员会主办、电子科技大学承办的全国大学生信息安全竞赛—创新实践能力赛（简称“大赛”），面向全国大学在校生开放。

大赛统一按照组建队伍在线报名、线上初赛、分区选拔赛、全国总决赛四个阶段组织相应类别的比赛。其中在线初赛由电子科技大学承办，永信至诚提供竞赛平台支撑；分区选拔赛分别由东北大学（东北赛区）、南开大学(华北赛区)、甘肃政法大学（西北赛区）、华中科技大学（华中赛区）、陆军工程大学（华东北赛区）、复旦大学（华东南赛区）、重庆邮电大学（西南赛区）、广东外语外贸大学(华南赛区）承办；全国总决赛由电子科技大学承办。

一、参赛对象及条件

全国高等学校（本科类和高职高专类院校）具有正规学籍的全日制在校大学生（包括高职高专、本科生、研究生）（含2019年应届毕业生），具体要求如下：

1、各参赛队伍学生通过竞赛网站注册 http://www.ciscn.cn/competition/securityCompetition?compet_id=29。

2、报名起止时间：2019年3月15日——2019年4月15日24时。

3、每个参赛队伍人数最多不超过6人，允许校内跨年级、跨专业组队，各高校参赛队数不限，不可跨校组队；

4、每人只能参加一支队伍（即个人参赛后不可再与他人组队参赛，或个人参加一个队伍后不可再参加另一个队伍），允许有一名指导老师；

5、高校在不同城市的校区视为不同高校，可分别组队参赛并入围到所在分区的分区选拔赛，以及总决赛阶段；

6、参赛者应保证报名信息的准确有效。分区选拔赛和总决赛时必须提供所在高校开具的学籍证明材料（纸质版）；评审时，如发现参赛队员不符合参赛规定，将取消参赛队伍的参赛或获奖资格；

7、指导教师必须是参赛队伍所在高校在职教师。指导教师可以指导学生进行组队、知识技能训练，但创新网络安全挑战设计、编程开发和现场参赛必须由参赛学生独立完成；

8、指导教师负责把握所指导学生参赛过程不违反比赛规则，不对比赛平台、系统和第三方服务进行攻击，以及不与国家法律、法规相违背；组委会将评选优秀指导教师（获得全国一等奖及创新单项奖团队的指导老师），并予以表彰。

二、线上初赛

1.线上初赛时间

2019 年 4 月 20 日 9：00——2019 年 4 月 21 日 9:00。

2.线上初赛入围规则

凡成功报名取得参赛资格的参赛队均自动进入线上初赛。即可获得参加线上初赛的资格。

3.赛题说明

线上初赛由大赛技术委员会命题，采用在线答题模式，题目覆盖多种创新实践能力基础技能，主要由知识问答模块和场景实操模块两部分组成。

（1）知识问答模块：以单项选择题和多项选择题方式考察，主要包括：意识形态安全、政策法规、安全防护、密码学、等级保护、安全运维、移动安全、网络安全、网络空间安全、数据库安全、云安全、大数据安全、密码学等知识。

（2）场景实操模块：覆盖 Web 安全、逆向分析、移动安全、二进制漏洞挖掘利用、密码学、信息搜集、编码分析、取证分析、隐写分析等技能范围。

4.计分规则

（1）采用动态 flag 反作弊监控技术，发现比赛作弊或对比赛平台攻击行为，将采取禁赛、直接取消比赛成绩等处罚措施，情节严重者将通报赛队所在高校；

（2）线上初赛后，要求各分区排名靠前的潜在入围分区赛的队伍在 8 小时内提交解题报告，由技术委员会进行审核，以确定比赛得分和排名；

（3）知识问答模块：采用在线考试方式，每支赛队报名参赛队员均需用独立账号参加作答，取赛队每位队员的平均分作为知识题的最终得分;

（4）场景实操模块：每题初始分值 500 分，采用动态积分方式（即题目分值随解出队伍数量增加而递减），并对前三支解出赛题的赛队进行动态分值 5%、3%、1%的奖励;

（5）参赛队需通过解题与技能实战获取得分，最终按知识问答模块*35%+场景实操模块*65%得出总成绩作为线上初赛最终得分。

5.晋级分区选拔赛规则

（1）参赛队需根据线上初赛最终得分在各分区排名，决出优胜入围各分区选拔赛的参赛队伍;

（2）线上初赛每个高校可以有多支队伍参加，最多有 2 支排名靠前的队伍晋级分区选拔赛;

（3）线上初赛在成绩排名相同且只有一个晋级名额的情况下，由研究生成员数较少的队伍晋级，如成绩仍然相同则由场景实操模块得分高的队伍晋级;

（4）线上初赛采取严格的反作弊监控机制，发现比赛作弊或对比赛平台攻击行为，将采取禁赛、直接取消比赛成绩等处罚措施，情节严重者将通报赛队所在高校。

三、分区选拔赛

1.分区选拔赛时间/地点

2019 年 5 月 22 日—2019 年 6 月 15 日期间，具体时间/地点/赛程安排另行通知给各分区入围分区选拔赛高校赛队。由大赛承办方统一提供附近宾馆、饭店等相关信息，食宿及相关费用由参赛学校自行安排。

2.各分区对应省市情况

东北赛区（辽宁、吉林、黑龙江）、华北赛区（北京、天津、河北、山西、内蒙）、西北赛区（陕西、宁夏、甘肃、青海、新疆）、华中赛区（河南、湖南、湖北）、华东北赛区（山东、安徽、江苏）、华东南赛区（上海、浙江、福建、江西、台湾）、西南赛区（重庆、四川、云南、贵州、西藏）、华南赛区（广东、广西、海南、香港、澳门）。

3.赛题说明

采用开放命题形式的创新实践能力挑战赛，由 Build（创新安全应用开发）、Break（安全应用攻击破解）、Fix（安全应用漏洞修补）三个环节构成。

（1）Build 环节：赛队根据技术委员会发布的应用场景开发功能与特性需求（包括二进制网络服务、Web 应用服务、移动 APP 及服务接口、物联网应用场景、逆向分析与移动安全），选择其中的场景，开发出符合所要求功能与特性的安全应用，并依据出题范围与难度要求预设创新性的网络安全挑战，构建出靶标环境。具体场景需求、功能接口、提

交靶标要求由技术委员会另行发布。技术委员会根据赛队提交靶标场景的难度、类型情况，可在某些方向上补充靶标环境，具体各个方向的题量、主要考察范围如下。

内容	主要考察范围
二进制网络服务	涉及 Linux 平台网络服务程序的设计、安全开发，以及二进制常见漏洞类型（如栈溢出、堆溢出、格式化字符串、UAF、竞争条件等）的原理与漏洞代码形态，漏洞挖掘及利用机制理解等
Web 应用服务	涉及 Windows、Linux 平台 Web 应用服务的设计、安全开发，以及 Web 应用服务常见漏洞类型（如 SQL 注入、XSS 跨站脚本、CSRF 跨站请求伪造、文件上传、文件包含、框架安全、越权、逻辑漏洞）原理与漏洞代码形态，漏洞挖掘及利用机制理解等
物联网场景	涉及物联网场景下 Web、APP、二进制程序的设计与安全开发，以及物联网场景常见漏洞的原理、挖掘与利用机制理解等
逆向分析与移动安全	涉及 Android、Linux 等平台的移动端 APP，及 Web 后台接口的设计与安全开发，要求利用常用工具对源代码及二进制文件进行逆向分析，掌握 Android 移动应用 APK 文件的逆向分析，掌握加解密、内核编程、算法、反调试和代码混淆技术等
密码学与杂项	涉及古典密码学、现代密码学、国密算法与信息搜集、编码分析、取证分析、隐写分析的综合应用等

（2）Break 环节（采用静态攻防）：技术委员会将根据靶标环境不在本赛队所在分区使用、不在不同竞赛时段重复使用的原则，从靶标候选库中抽取部分优秀靶标作为 Break 环节的赛题使用，其他的赛题将由技术委员会命题。

内容	主要考察范围
二进制网络服务	涉及 Linux 平台网络服务程序常见漏洞类型(如栈溢出、堆溢出、格式化字符串、UAF、竞争条件等）的挖掘及利用技术等
Web 应用服务	涉及 Windows、Linux 平台 Web 应用服务常见漏洞类型（如 SQL 注入、XSS 跨站脚本、CSRF 跨站请求伪造、文件上传、文件包含、框架安全、越权、逻辑漏洞）的渗透测试、代码审计及漏洞利用技术等
物联网场景	涉及物联网场景下 Web、APP、二进制程序的渗透及逆

	向分析，以及物联网场景漏洞的挖掘与利用技术等
逆向分析与移动安全	涉及 Android、Linux 等平台的移动端 APP，及 Web 后台接口渗透测试及逆向分析，移动场景的安全漏洞挖掘与利用技术
密码学与杂项	涉及古典密码学、现代密码学、国密算法与信息搜集、编码分析、取证分析、隐写分析的综合应用等

（3）Fix 环节（采用静态攻防）：各赛队对靶标环境进行漏洞修复。

内容	主要考察范围
二进制网络服务	涉及 Linux 平台应用二进制漏洞机理理解，挖掘与修补技术等
Web 应用服务	涉及 Windows、Linux 平台 Web 应用服务常见漏洞类型的机理理解，挖掘与修补技术等
移动 APP	涉及 Android、Linux 等平台的移动端 APP，及 Web 后台接口渗透测试及逆向分析，移动场景的安全漏洞机理理解，挖掘与修补技术
物联网场景	涉及物联网场景的漏洞机理理解，挖掘与修补等

4.计分规则

分区选拔赛各赛队排名按照 Build、Break、Fix 三个环节得分总和进行排名，Build、Break、Fix 三个环节各占权重比例为 20%:60%:20%。

（1）Build 环节

1、晋级队伍需要在第一周(第 1-7 日)之内提交自行创新赛题的源码、设计文档、视频演示、题目提示、EXP 脚本、Checker 脚本等至技术委员会提供的邮箱，提交后将按照提交时间进行编号，由技术委员会负责审核。参赛队伍如若发现赛题存在问题，可在随后的一周(第 8-14 日)内向技术委员会申请更新赛题，每个队伍仅允许更新一次赛题；

2、第一周没有提交而第二周才提交赛题者该环节得分将扣 5 分，不提交赛题的队伍该环节得分为 0。赛题若存在高度雷同的情况下，将直接通报大赛组委会，该环节得分为 0；

3、赛队在 Build 环节得分按照：功能实现度（占%60）+EXP 通过率（占 10%）+能力符合度（占 10%）+选中作为大赛赛制（占 20%）综合计分。

功能实现度评价：赛队提交靶标环境后，靶标环境进入候选靶标库，由技术委员会使用 Checker 程序进行测试，根据通过功能特性测试的比例，给出功能实现度评价。

通过率评价：对参赛队伍提供的 EXP 脚本进行预设创新性网络安全挑战测试，以能成功获取平台方配置的 Flag，给出 EXP 通过率评价。

能力符合度评价：按照每个靶标环境被其他赛队解出的次数是否符合预期的难度，给出能力符合度评价。

（2）Break 环节

1、各赛队对抽取的靶标环境进行预设安全挑战研究与破解，尝试检测出靶标环境中的预设安全挑战或者未预期安全漏洞，攻破靶标环境获取 Flag 进行得分，每个靶标环境初始分值 500 分，采用动态积分方式（即题目分值随解出队伍数量增加而递减），并对前三支解出赛题的赛队进行动态分值 5%、3%、1%的奖励；

2、Break 环节各赛队得分，为各队在比赛时间内解出靶标环境安全挑战所得分的总和；每个赛队与该分区选拔赛队 Break 环节最高分的比值 * Break 环节权重分，得到各赛队在 Break 环节得分。

（3）Fix 环节

1、 Fix 环节结束后，由赛事组织方采用 EXP 和 Checker 脚本对队伍修补靶标进行测试，保证 Checker 通过（或不低于初始功能实现度）而 EXP 不成功，则为修补成功，否则修补失败。每个靶标环境初始分值 500 分，采用动态积分方式（即题目分值随成功修补队伍数量增加

而递减），分值范围为 100-500 分，并对前三支成功修补赛题的赛队进行动态分值 5%、3%、1%的奖励；

2、 Fix 环节各队伍得分，为各队在比赛时间内成功修补靶标环境得分的总和，与该分区选拔赛队 Fix 环节最高分的比值 *Fix 环节权重分，得到各队在 Fix 环节得分。

5.晋级规则

（1）分区选拔赛时必须提供所在高校开具的学籍证明材料（纸质版）；评审时，如发现参赛队员不符合参赛规定，将取消参赛队伍的参赛或获奖资格；

（2）分区赛场上允许不超过 4 名队员，2 名队员在场边候补，可由指导老师或场上队长申请替补上场；

（3）分区赛入围名额根据各自分区报名赛队数量和承办高校场地条件由各承办高校确定，原则上每个赛区取 24-50 支队伍晋级分区选拔赛；

（4）分赛区在成绩排名相同且只有一个晋级全国总决赛名额的情况下，由研究生成员数较少的队伍晋级；

（5）比赛过程中不允许参赛队使用手机、即时通信软件等渠道与外界沟通交流，采取比赛平台严格的反作弊监控机制，赛后要求排名靠前潜在入围总决赛的赛队在 1 小时内提交解题报告由技术委员会进行审核，以确定比赛得分和排名；

（6）对于过程中发现比赛作弊或对比赛平台攻击行为，将采取禁赛、直接取消比赛成绩等处罚措施，情节严重者将通报赛队所在高校。

四、全国总决赛

1.全国总决赛时间/地点

2019 年 7 月 27 日-2019 年 7 月 28 日，电子科技大学，详细时间/地点/赛程安排另行通知给全国总决赛入围高校赛队。全国总决赛时，由大赛承办方统一提供附近宾馆、饭店等相关信息，食宿及相关费用由参赛学校自行安排。

2.赛题说明

总决赛采用开放命题形式的攻防竞赛形式，由 Build（创新安全应用开发）、Break & Fix（攻击、防御综合对抗）两个环节各占权重比例分别为 20%、80%。Share（创新思路分享）环节单独评分并设单项奖。

（1）Build 环节：要求及计分规则与分区选拔赛相同。技术委员会根据赛队提交靶标场景的难度、类型情况，可在某些方向上补充靶标环境以及基于场景的赛题。

（2）Break & Fix 综合攻防环节（采用动态攻防）：综合攻防环节中各参赛队伍同时进行 Break 安全应用攻击破解和 Fix 安全应用漏洞修补的操作，并采用“零和游戏”计分规则进行计分与排名。

3.计分规则

全国总决赛各赛队排名按照 Build、综合对抗（Break&Fix）两个环节得分总和进行排名，Build、综合对抗（Break&Fix）各占权重比例为 20%:80%。

（1）Build 环节得分根据占总分 20%的比例，在综合对抗环节开始前计入最终总分。

（2）综合对抗环节采用“零和游戏”计分规则进行计分与排名。技术委员会选取参赛选手 Build 环节评分高的赛题和技术委员会出的基于场景的赛题。参赛队对其他队伍的靶标环境进行研究破解，尝试检测出靶标环境中的安全挑战或者未预期安全漏洞，攻破靶标环境获取 Flag 进行得分，被攻破方相应减分，或者通过协议拒绝服务漏洞攻击使得靶标环境中服务不正常，使得被攻击方减分，平分给服务正常的赛队；参赛队对己方靶标环境所遭受的攻击流量 PCAP 文件进行监测分析，尝试找出对手攻击行为模式，并通过设置规则进行阻断，以避免被攻击失分；比赛最后阶段放开队伍对己方靶标环境的访问权限，赛队对靶标环境进行漏洞修复、后门识别移除等防御动作，同时各赛队继续攻防对抗操作。如赛队预设创新安全挑战的靶标环境未被任何其他赛队攻破获得 Flag，则其初始分值一定比例将平分给所有赛队。

（3）Share 环节：参赛队提交创新安全挑战设计报告，分享创新安全挑战设计思路，以及综合环节创新性的思路技巧，接受评委和其他赛队质疑，由评委进行打分。该环节得分不计入竞赛分，只用于评选创新网络安全挑战单项奖。

4.晋级规则

（1）全国总决赛时必须提供所在高校开具的学籍证明材料（纸质版）；评审时，如发现参赛队员不符合参赛规定，将取消参赛队伍的参赛或获奖资格；

（2）总决赛场上允许不超过 4 名队员，2 名队员在场边候补，可由

指导老师或场上队长申请替补上场；

（3）比赛过程中不允许参赛队使用手机、即时通信软件等渠道与外界沟通交流，采取比赛平台严格的反作弊监控机制，赛后要求排名靠前潜在入围总决赛的赛队在 1 小时内提交解题报告由技术委员会进行审核，以确定比赛得分和排名；

（4）对于过程中发现比赛作弊或对比赛平台攻击行为，将采取禁赛、直接取消比赛成绩等处罚措施，情节严重者将通报赛队所在高校。

五、奖项设置

1.选拔赛奖项

（1）分区选拔赛成绩排名前 4 名的队伍获得晋级全国总决赛；

（2）分区的成绩排名前 4 名~前 20%中遴选其他进入全国总决赛名额，这些队伍中进入总决赛的队伍同时获得赛区特等奖，其余未进入总决赛的队伍按照最低分数达到一定上限后，获得全国三等奖&赛区一等奖；

（2）分区选拔赛成绩排名前 20%~前 40%的队伍获得赛区二等奖；

（3）分区选拔赛成绩排名前 40%~前 60%的队伍获得赛区三等奖；

（4）得到教育厅对赛事级别认同的省/直辖市/自治区，如没有参赛队伍获得赛区奖项，其成绩最高的团队可获得赛区三等奖。

2.全国总决赛奖项

（1）总决赛成绩排名前 3 名的队获得全国特等奖；

（2）总决赛成绩排名前 3 名~前 40%的队获得全国一等奖；

（3）总决赛成绩排名前 40%~80%的队获得全国二等奖；

（4）总决赛成绩排名 80-90%的队获得全国三等奖；

（5）总决赛成绩排名 90%之后的队获得优胜奖；

（6）技术委员会根据情况评选 10%-20%队授予网络安全挑战创新单项奖；

（7）在相同成绩相同排名并且需要决出一个获奖名额的情况下，由研究生成员数较少队伍获胜，如仍不能决出则由组委会评判；

（8）大赛颁发统一的获奖证书，对获奖参赛队伍予以奖励，由教育部高等学校网络空间安全专业教学指导委员会负责颁奖事宜；

（9）所有获奖队伍及名单将以多种方式公布，并报送相关高校，作为高校评定奖学金、推荐研究生等的参考；

（10）获奖队伍必须参加第十二届全国大学生信息安全竞赛-创新实践能力赛颁奖大会。

六、违规处理

以下情况将视为违规，大赛组织委员会视情节严重程度追究违规方责任，直至取消责任方参赛资格：

（一）针对参赛队伍的禁止项：

1、参赛报名信息作弊或造假的行为；

2、在参赛过程中出现违反相关法律、法规的行为；

3、涉嫌抄袭、代打、串题等作弊行为；

4、攻击比赛平台或在规则之外恶意攻击其他竞赛选手，破坏比赛公平性、稳定性的行为；

5、在比赛过程中发现或者被举报认定存在的其他违规行为。

（二）针对承办院校与大赛平台支持厂商的禁止项：

1、平台未提供必要的防作弊功能，严重影响大赛公平的；

2、大赛组织不力，缺少裁判机制或出现裁判不公情况的；

3、未遵守赛题管理要求，导致漏题泄题事故的。

七、申诉与仲裁

1、参赛团队或选手对不符合大赛规定的、有失公正的评判和奖励以及工作人员的违规行为等，均可向大赛组委会提出申诉（邮箱：cxsjnlszc2019@163.com）。组织委员会负责受理比赛中提出的申诉并进行调解仲裁，以保证大赛的顺利进行和大赛结果的公平公正。组织委员会作出的仲裁结果为终局决定。

2、申诉报告应明确申诉内容，指定一名成员作为联系人，并有参赛队伍成员的签名，否则申诉将不予受理。

3、组织委员会将在收到申诉报告之日起10个工作日内予以受理，并认真审核和处理。

八、联络信息

大赛期间，具体活动时间具体计划以官网公布为准。

联系人：文老师 18108272477、何老师 18080139930

电子邮箱：cxsjnls12@163.com

九、其他

本大赛规程的最终解释权归第十二届全国大学生信息安全竞赛—

创新实践能力赛组委会所有。

教育部高等学校网络空间安全专业教学指导委员会

第十二届全国大学生信息安全竞赛-创新实践能力赛组委会

2019 年 4 月 7 日