2020 年第 17 届全国大学生信息安全与对抗技术竞赛通知

(ISCC2020)

1 竞赛简介

信息安全已涉及到国家政治、经济、文化、社会和生态文明的建设，信息系统越发展到它的高级阶段，人们对其依赖性就越强，从某种程度上讲其越容易遭受攻击，遭受攻击的后果越严重。“网络安全和信息化是一体之两翼、驱动之双轮。没有网络安全就没有国家安全。”信息是社会发展的重要战略资源，国际上围绕信息的获取、使用和控制的斗争愈演愈烈，信息安全保障能力是综合国力、经济竞争实力和生存能力的重要组成部分，是世纪之交世界各国奋力攀登的至高点。

信息安全与对抗技术竞赛（ISCC：Information Security and Countermeasures Contest），于 2004 年首次举办（国内第一），2020 年为第 17 届。2019 年竞赛的注册人数近 **7000** 人，参加竞赛的院校数 **1000** 多所，ISCC 竞赛的影响广泛且深远。竞赛不断追求“更高、更快、更强”，持续培养高素质信息安全对抗专业人才。

2 竞赛宗旨

全面贯彻国家关于网络安全和信息化工作的重要精神，提升信息安全意识，普及信息安全知识，实践信息安全技术，共创信息安全环境，发现信息安全人才！

3 竞赛形式

竞赛包括 3 项：个人挑战赛、分组对抗赛和无限擂台赛。

个人挑战赛采取线上模式，题目类型包括 CHOICE、BASIC、WEB、REVERSE、PWN、MISC 和 MOBILE 等，同时增加了组合题目的形式。

1. CHOICE:涉及信息安全多类知识点，适合刚接触信息安全人士的学习。
2. BASIC: 信息安全基础知识，普及信息安全知识，引导信息安全爱好者入门。
3. WEB: 考察 sql 注入、跨站脚本攻击、上传漏洞攻击以及 PHP 代码审计等知识，题目有时会结合其他题型。
4. REVERSE: 考察逆向破解能力，需要熟练地掌握汇编语言。

5. PWN: 考察软件漏洞挖掘与利用能力，需要较好的掌握操作系统原理。
6. MISC: 考察隐写术、流量分析、内核安全等技术。
7. MOBILE:考察移动终端安全攻防能力。
8. 组合题目：由同种类型或不同类型的 2 道或 3 道题目串联而成。如果无法获得前边题目的提示信息，则很难解出后面题目的 flag。组合题目的题目格式为“xxx-1”、“xxx-2”、“xxx-3”。

分组对抗赛为线下模拟环境中的真实对抗，主要采取阵地夺旗、占领高地等模式进行攻防比拼。比赛时，各队伍通过对指定的服务器进行入侵攻击达到获取旗子的目标而得分，并在攻上高地后防御其他队伍的攻击。

无限擂台赛主要面向基础知识扎实，做题经验丰富或极具创新思维的选手。选手通过解答擂台上的题目来获得打擂的资格，通过提交原创题目并通过主办方的审核后，取代擂台上的题目实现成功打擂。擂台题目会根据在擂台上未被解出的持续时间获得加分，持续时间越长，获得的分数越多。

4 参赛方式

个人挑战赛和无限擂台赛不仅面向在校学生，还面向社会各界人士，人数不限，选手可进入本次竞赛入口（http://www.isclab.org.cn）进行注册参赛。本次竞赛暂不接受组队参赛。注意，用户名、队伍等注册信息中，请勿出现暴力、色情、政治等相关表述，如发现将删除账号。

分组对抗赛则采取选拔个人挑战赛中的优秀选手和各赛区推荐部分选手，每组 3 人。

5 竞赛日程

个人挑战赛与无线擂台赛将于 2020 年 5 月 1 日上午 8：00 开始，一般持续 25 天左右。

分组对抗赛将于个人挑战赛及无限擂台赛结束后于暑期进行，一般持续 2 天，时间一般安排在 7 月中旬，暂定竞赛地点为北京理工大学。

6 竞赛评测

6.1 个人挑战赛

个人挑战赛评奖采用积分制，参赛选手按分数的多少进行排序，竞赛评分以选手攻关数目多少和系统记录的过关时间先后为依据。选手的最终成绩为通过各关所获分数的累积。选手按分数多少排序，两名选手得分相同时，则查看各自通过最后一关的时间，先通过者优于后通过者。最后按照名次先后进行评奖。

1. 线上初赛题目会根据时间安排以及选手的解题进度由组委会逐步开放。
2. 线上赛答题方式为提交 flag，由系统自动审核。
3. 线上赛每题分值从 50-500 分不等，分值信息会在具体题目中给出。
4. 积分相同时，根据最后一道得分题目提交时间，先提交者名次高。
5. 若某道题目没有选手能解出时，组委会将适时发布提示信息。
6. 选手若发现竞赛平台或者赛题有非预期漏洞并通报组委会时，组委会会酌情加分。
7. 禁止对赛题以外的平台发起攻击，违规者一律取消参赛资格。

6.2 分组对抗赛

分组对抗赛视当年题目性质评定分数，有加分和减分项。

1. 禁止参赛队之间分享任何解题思路及 flag，违规者一律取消参赛资格。
2. 禁止任何对比赛平台的暴力破解，违规者一律取消参赛资格。
3. 禁止对赛题以外的比赛平台发起攻击，违规者主页取消参赛资格。

6.3 无限擂台赛

评奖采用评分制，参赛选手按分数的多少进行排序，竞赛评分以选手得分及打擂成功的先后顺序为依据。选手的最终成绩为解答题目与原创题目所获分数的累积。选手按分数多少进行排序，两名选手得分相同时，则查看各自第一次打擂成功的时间，先成功者优于后成功者。

1. 擂台赛首先由主办方放出第一轮擂台题目，之后由选手进行打擂、上传。题目分为 WEB、REVERSE、MISC、MOBILE、PWN 五种类型，每种类型一个擂台。

2. 选手正确解出擂台上某种类型的题目后，获得 150 答题分，之后可以向组委会邮箱发送自己设计的同种类型的题目。待组委会审核通过后即可替换擂台题目，即视为打擂成功。
3. 擂台上每道题目的得分随时长而增加，3 小时内无人解出可获得 300 分，6 小时内无人解出可获得 450 分。计时为题目开放初始时间至有选手正确提交 flag 为止。如果超过 3 天时间无人解出，将会放出解题提示。
4. 打擂邮件的主题为“题目类型+选手注册 id”，审核顺序为邮件接收的顺序而非提交擂台题目 flag 的顺序，一旦有题目符合要求，审核通过，替换擂台中的题目（即打擂成功），则其余选手本轮打擂提交的题目不再审核，选手可留至下一轮打擂解出 flag 后再次提交。每日审核的题目为前一天 0~24 点发送的题目。
5. 擂台赛答题方式为提交 flag，由系统自动审核，flag 正确即可进行原创题目的提交。提交题目的时间不得早于系统记录的该选手提交同类型题目的 flag 的时间。组委会替换擂台题目的时间为每天 15 点。
6. 选手提交题目的材料需包括所有的源码文件及 flag 信息、详尽的 writeup 及解题用到的脚本，以及题目部署方式的文档等，具体内容参见“**ISCC 擂台赛出题模板**”。缺少有关信息将不会审核通过。
7. 同一选手可同时在多个擂台进行打擂。最终擂台赛成绩为所有题目得分的累加和。
8. 选手发现擂台上的题目有漏洞或其他错误可通过邮件或 qq 群进行反映，组委会将酌情扣除该题目质量的得分。
9. 选手题目如包含需暴力破解或其他不符合竞赛内容的题目将不会审核通过。
10. 所有题目均需选手原创，一经发现雷同或其他作弊行为将严肃处理。
11. 禁止对赛题以外的平台发起攻击，禁止在提交的赛题中隐藏后门，违规者一律取消参赛资格。
12. 本届擂台赛为第一次举办，具体规则在比赛期间可能会有变动，请各位选手注意关注竞赛网站通知。

7 联系方式

竞赛入口：http://www.isclab.org.cn

竞赛邮箱：iscc2004@163.com

竞赛组 QQ 群：876290071（1 群）、786047411（2 群）、1025258470（3 群）（供参赛者进行技术交流，严禁剧透）

8 组织单位

主办单位：

中国兵工学会

中国兵工学会信息安全与对抗专业委员会

承办单位：

北京理工大学信息系统及安全对抗实验中心

协办单位：

广西壮族自治区科学技术协会

广西信息安全学会

河南省科联电子科技有限公司

北京大学软件学院信息安全团队

公安部第三研究所《信息网络安全》杂志社

9 其他事项

1. 竞赛旨在普及信息安全知识，引导初学者进行学习，并为技术爱好者们提供一个交流的平台。恶意攻击竞赛服务器的参赛者将失去比赛资格。
2. 竞赛的最终解释权归“信息安全与对抗技术竞赛组委会”所有。

10 FAQ

1. 什么是 ISCC?

   ISCC 是 Information Security and Countermeasures Contest（信息安全与对抗技术竞赛）的缩写，每年举办 1 届，2004 年举办第 1 届竞赛，2020 年为第 17 届竞赛。ISCC 由北京理工大学罗森林教授提出，最早由北京理工大学教务处主办，而后由教务处、网络中心、团委共同主办。截止目前已有多家主办、协办和支持单位，其

宗旨是面向广大民众：提升信息安全意识，普及信息安全知识，实践信息安全技术，共创信息安全环境，发现信息安全人才。

ISCC 分为二个阶段，即“个人挑战赛及无限擂台赛”和“分组对抗赛”。

2. 什么是 CTF（Capture The Flag）？

CTF 夺旗赛是信息安全竞赛的一种形式，flag 是指一串字符信息，它可能会被放在远程服务器上，也可能会被加密和隐藏在各种不容易访问到的媒介上，参赛选手通过使用逆向、解密、取证分析、渗透利用等技术来拿到 flag。

CTF 夺旗赛通常有两种形式，解题模式（Jeopardy）和攻防模式（Attack-Defense）。

（1）解题模式中，通过一系列不同类型的赛题，比如给定一个有漏洞的服务、提供一段网络流量、给出一个加密后的数据等，将 flag 隐藏在这些题目中，选手们通过解题获得积分。

（2）攻防模式中，通过事先给定一个接近真实的具有系列漏洞的服务环境，每个参赛队都具有相同的环境，参赛队一方面需要修补自己服务的漏洞，同时也需要去攻击对其他参赛队的服务，获得他人环境中的 flag 来得分，比赛过程也更加激烈。

3. 竞赛题目有哪些类型？难度如何？

ISCC 题目涉及面较广，包含但不限于 Web 渗透、漏洞挖掘与利用、加密解密等。ISCC 题目难度差异很大，一方面，面向尽可能多的参赛选手，都有一定的参与机会和效果。另一方面，面先优手选手提供更能充分发挥其能力的题目。

4. 我能参加 ISCC 吗？如何报名？

任何人都可以参加 ISCC，个人挑战赛及无限擂台赛仅需于网站注册账号即可参赛。分组对抗赛采用选拔和邀请模式。

全国大学生信息安全与对抗技术竞赛组委会