



# 信息安全与对抗技术竞赛组委会

## ISCC 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, 2004 年为首届竞赛, 每年举办一届。

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。

ISCC 宗旨: 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。

### 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, 也可能被加密和隐藏在各种不容易访问到的媒介上, 参赛队通过使用逆向、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, 参赛队通过解题获得积分。(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, 不同赛项的题目类型如下:

破阵夺旗赛和无限擂台赛中, 题目类型包含 CHOICE、WEB、REVERSE、PWN、MISC 和 MOBILE 等。

数据安全赛中, 参赛队使用机器学习、深度学习方法对题目中描述的应用问题进行建模, 并提交对测试数据集的预测结果。

博弈对抗赛中, 参赛队除了解答包含 CHOICE、REVERSE、MISC 和 MOBILE 等类型的题目外, 还将进行阵地夺旗、占领高地等模式的攻防比拼。

智能安全赛中，参赛队可参与空地协同应用、工业互联网、仿人智能体、城市道路自动驾驶、自动驾驶仿真、采收机器人、植保机器人、灌溉机器人、授粉机器人、复合智能体、看护机器人、药房机器人等赛道。

ISCC 题目难度差异很大，一方面，面向尽可能多的参赛队伍，都有一定的参与机会和效果。另一方面，面向优秀队伍提供更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。其中，破阵夺旗赛、无限擂台赛及数据安全赛仅需在网站注册账号即可参赛，博弈对抗赛采用选拔和邀请的模式。

#### **5 是否有往届赛题或训练平台？**

ISCC 竞赛组委会为参赛队提供了常态化在线 CTF 系统和数据安全赛练习系统，系统设计的目的是让参赛队有充足的时间了解比赛模式、熟悉比赛流程和快速学习比赛内容等。详见官网：[www.isclab.org.cn](http://www.isclab.org.cn)。

常态化在线 CTF 系统设有挑战题模块和积分榜模块。挑战题模块设置了 WEB、REVERSE、PWN、MISC 和 MOBILE 等对应练习板块。各个板块所包含的练习题为 ISCC 近年来的高水平赛题，旨在让参赛队在学有所获的过程中感受历年 ISCC 比赛的风采。同时，CTF 练习系统也设有与破阵夺旗赛中相同的积分榜模块，参赛队可以从中了解自己的水平定位，并查看可视化的做题历程。

数据安全赛练习系统将提供历届的赛题作为习题。参赛队可以根据题意解题，在系统上提交预测结果。在该系统中，仅保留 A 榜的评价预测结果，参赛队可实时获知预测结果的准确性。