

关于举办第十五届广东大学生科技学术季 活动之第二届广东大学生网络安全攻防 大赛的工作方案

没有网络安全就没有国家安全，没有信息化就没有现代化。为深入学习贯彻习近平总书记关于网络安全和信息化工作的重要指示批示精神，为国家安全、网络安全培育青年人才，根据《关于举办第十五届广东大学生科技学术季活动的通知》的要求，现将第二届广东大学生网络安全攻防大赛有关事项安排如下。

一、比赛主题

国家安全 青年担当

二、活动时间

2022年3月至6月

三、组织机构

（一）主办单位：共青团广东省委员会、广东省教育厅、广东省科学技术厅、广东省科学技术协会、广东省学生联合会

（二）承办单位：惠州学院

（三）技术指导：广东省网络空间安全产业创新联合会

（四）平台技术支持：奇安信科技集团股份有限公司

大赛设立组委会，由主办、承办单位的有关负责人组成，负责比赛组织领导工作。组委会下设办公室，设在惠州学院

团委，负责比赛日常事务。大赛设立评委会，由组委会聘请各领域学术专家组成，负责参赛作品的评审工作。

四、参赛对象

活动面向全省高校全日制在校大专生、本科生、研究生。

1.每个参赛队伍人数不超过4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；

2.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），每支队伍可配1-2名指导老师；

3.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，但现场参赛必须由参赛学生独立完成；

4.指导教师负责全程管理、指导参赛的学生队伍，参赛过程不得违反比赛规则，不对比赛平台、系统和第三方服务进行攻击，不得与国家法律、法规、公序良俗相违背（如队名等）。

五、比赛时间与地点

（一）日程安排

1.4月15日前，各高校开展我国第七个“4·15”全民国家安全教育日系列活动：举办主题团日活动、主题宣传讲座、社团主题培训，发布专栏推文、观看宣传教育短片、主题演讲等，突出校园主阵地开展国家安全观、网络安全观主题宣传；

2.4月15日，第二届广东大学生网络安全攻防大赛正式

启动；

3.5月15日前，各高校遴选参加全省比赛队伍，一所学校可有多组队伍参赛；

4.5月21日至22日，组织省级初赛评审，初赛内容为30%知识赛+70%攻防夺旗赛，按照成绩高低取前30名队伍进入省级总决赛，每个高校晋级队伍不超过2个；

5.5月28日至29日，组织省级总决赛评审，总决赛内容为现场攻防赛。举办网络空间安全前沿技术高峰论坛（专家讲座暨颁奖典礼）；

6.6月11日至6月12日，组织获奖优秀选手参观行业顶尖的网络空间安全企业，并举行“青马红客100”交流活动，组织“青马红客100”学员与获奖选手交流。

（二）省级决赛地点

惠州学院

六、比赛内容

比赛将采用安全基础知识普及，CTF夺旗赛、AWD攻防、综合渗透赛等赛制。在成熟的赛制下，通过提高题目质量、丰富题目内容、创新题目类型，力争完成一次让选手满意、具有社会知名度的网络安全大赛。

比赛形式为三个阶段：

第一阶段：线上知识赛（30%）

比赛时长为2小时。主要考查参赛选手的安全理论知识。理论知识主要包括法律法规、网络安全基础知识和安全运维知识。

第二阶段：线上晋级赛（70%）

比赛时长为 8 小时。晋级赛制为 CTF 夺旗赛模式，CTF 夺旗赛模式提供一系列不同类型的赛题，比如上线一个有漏洞的服务、提供一段网络流量、给出一个加密后的数据或经过隐写后的文件等，参赛选手通过解题获得相应题目中的 flag（旗标文件），并提交至评分系统，评分系统审核确认 flag 正确后，将自动将积分传递给选手，以获得相应的分值。

第三阶段：线下省级总决赛

比赛时长为 4 小时。线下总决赛为 AWD 攻防模式，参赛队伍在网络空间互相进行攻击和防守，挖掘网络服务漏洞并攻击对手服务来得分，修补自身服务漏洞进行防御来避免丢分。攻防模式可以实时通过得分反映出比赛情况，最终也以得分直接分出胜负，是一种竞争激烈，具有很强观赏性和高度透明性的网络安全赛制。在这种赛制中，不仅仅是比参赛队员的智力和技术，同时也比团队之间的分工配合与合作。

序号	名称	晋级比例	考核内容
1	线上知识赛		法律法规、网络安全基础知识和安全运维知识
2	线上晋级赛		WEB、CRYPTO、PWN、REVERSE、MISC
3	线下总决赛	30 支队伍	WEB 安全、渗透测试、攻击与防御

七、奖项设置

本比赛为团队赛，依照实际参赛队伍确定奖项：

特等奖占比 5%，一等奖占比 15%，二等奖占比 30%，三等奖占比 50%，小数点后四舍五入。获得二等奖及以上的参赛队指导教师获“优秀指导教师”。此外，获得三等奖及以上的优秀选手被列入“青马红客 100”广东青年大学生网络空间安全人才培养计划人才库，获得二等奖及以上的优秀选手将获得“青年红客 100”相关优质网络安全领域单位提供的实习机会，评价为优秀的可获得校招就业机会。

八、报名时间与方式

报名时间：截止至 2022 年 5 月 15 日（星期日）17:00。

报名方式：参赛学校填写相关报名表，将省级初赛报名表（附件 3）发至指定邮箱 tw@hzu.edu.cn；同时，加入赛事咨询 QQ 群 825405920。

（一）团省委学校部

联系人：王梓

联系电话：020—87195615

（二）惠州学院

联系人：邓璐

联系电话：0752-2529160

邮 箱：tw@hzu.edu.cn

地 址：惠州市惠城区演达大道 46 号

附件：1.第二届广东大学生网络安全攻防大赛赛事安排
2.第二届广东大学生网络安全攻防大赛任务书
（样题）

3.第二届广东大学生网络安全攻防大赛报名表

第十五届广东大学生科技学术季活动组委会办公室
(省学联秘书处代章)

2022年3月17日

附件 1

第二届广东大学生网络安全攻防 大赛赛事安排

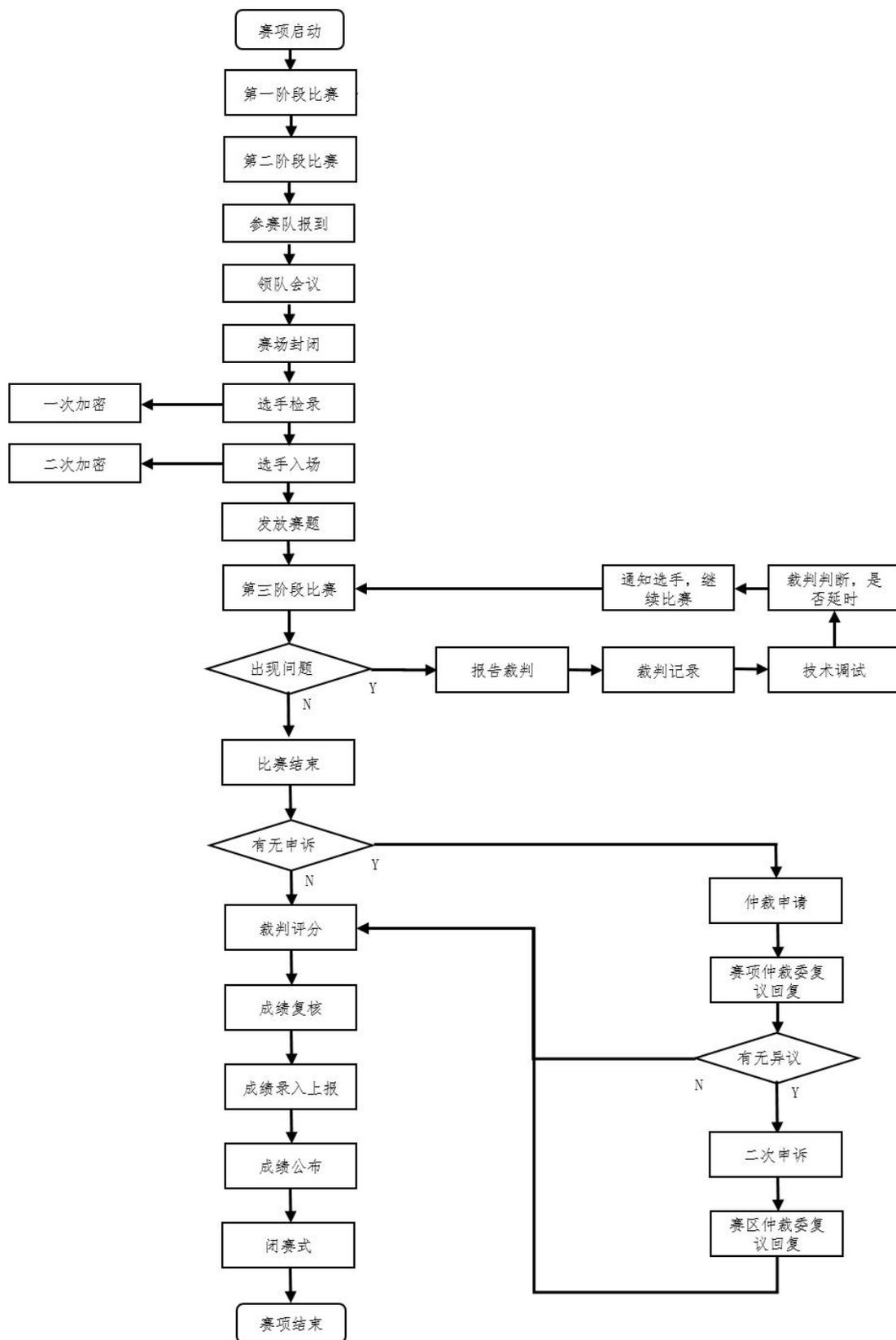
一、比赛时间安排表

线上资格选拔和晋级赛分别进行，总决赛限定在 1 天内进行，具体安排如下：

日期	时间	事项	参加人员	地点
5 月 21 日	10:00-12:00	线上选拔赛	参赛队	线上
5 月 22 日	9:00-18:00	线上晋级赛	参赛队	线上
5 月 28 日	09:00-14:00	参赛队报到，安排住宿，领取资料	工作人员、参赛队	住宿酒店
	09:00-12:00	裁判培训会议	裁判长、裁判员、监督组、专家组	会议室
	13:00-14:00	裁判工作会议	裁判长、裁判员、监督组	会议室
	14:00-15:00	领队会	各参赛队领队、裁判长	会议室
	15:00-16:00	开赛式	领导、各参赛队领队、参赛选手、裁判长、裁判、监督、仲裁	会议室

	16:00-17:00	熟悉赛场	各参赛队领队、参赛选手	比赛场地
	17:15	检查封闭赛场	裁判长、监督组	比赛场地
5月29日	07:30	参赛队到达比赛场地前集合	各参赛队、工作人员、裁判就位	比赛场地
	07:30-08:00	第一次抽签加密(抽序号)	参赛选手、裁判	比赛场地
	08:00-08:30	第二次抽签加密(抽工位号)	参赛选手、裁判	比赛场地
	08:30-08:40	参赛选手就位,宣读考场纪律	参赛选手、裁判	比赛场地
	08:40-09:00	设备工具检查确认、题目发放	参赛选手、裁判、监督、仲裁	比赛场地
	09:30-13:30	参赛队比赛	参赛选手、裁判、监督、仲裁	比赛场地
	13:30-15:00	申诉受理	参赛选手、裁判、监督、仲裁	比赛场地
	15:00-17:00	评分核分、抽检复核、解密	裁判、监督	判分会议室
		网络空间安全前沿技术高峰论坛	领导、各参赛队	
	17:00-17:30	闭赛式(宣布成绩、颁奖)	领导、嘉宾、裁判、各参赛队	指定的会议室

二、比赛流程图



附件 2

第二届广东大学生网络安全攻防大赛

任
务
书

(样题)

赛位号: 1-1

第一部分比赛设备及注意事项

一、注意事项

比赛分三个阶段依次晋级进行，第一第二阶段为线上赛，第三阶段为线下省级总决赛。

二、硬件环境

序号	设备名称	单位	数量
1	网络安全竞技平台 参数：奇安信网络安全竞技平台 GFW-AS-810-PA-01 为 2U 设备，标配 2 个千兆以太网口，Intel 处理器，256G 内存，SAS 硬盘。 提供选择题、CTF 题、攻防题赛题类型，支持攻防态势展示，提供符合行业场景的攻防对抗靶场环境。	台	1
2	电脑参数建议：CPU 主频 $\geq 2.8\text{GHZ}$ ， \geq 四核四线程；内存 $\geq 8\text{G}$ ；硬盘 $\geq 500\text{G}$ ；尺寸硬件虚拟化。	台	选手自备

第二部分比赛任务

任务一：

一、任务要求

第一阶段：线上知识赛，理论答题。（30%）

第二阶段：线上晋级赛，CTF 夺旗模式。（70%）

第三阶段：线下总决赛，AWD 混战模式。

二、任务环境

1.每参赛队选手每人分配一台客户机，比赛系统地址和测试系统账号密码，以比赛现场发放为准；

2.本次比赛采用统一网络环境比赛，请不要随意更改测试客户端的网络地址信息，对于更改客户端信息造成的问题，由参赛选手自行承担比赛损失；

3.请不要恶意破坏测试环境，对于恶意破坏测试环境的参赛者，组委会根据其行为予以处罚直至取消比赛资格。

4.比赛过程中及时保存相关文档；

5.比赛相关文档中不能出现参赛学校名称和参赛选手名称，以赛位号（工位号）代替；

6.参赛选手请勿删除模板内容，若因删除导致任何问题后果自负；

7.若同一文档由不同选手完成，须将文档合并后作为最终结果提交到 U 盘中；

8.比赛中出现各种问题及时向监考裁判举手示意，不要

影响其他参赛队比赛。

三、任务说明

第一阶段：线上知识赛

1.SQL 注入攻击的基本思路是（ ）

A 查找可疑注入点，验证注入点，利用注入点执行 SQL 命令

B 本地搭建数据库，登录数据库，执行 SQL 命令

C 搜集数据库服务器，爆破口令

D 询问管理员账号密码

2.在 windows 系统下，添加隐藏用户该使用下列哪一条命令（ ）

A net user admin admin\$ /add

B net user admin\$ admin\$ /add

C net user admin\$ admin123

D net user admin admin123

第二阶段：线上晋级赛

1.PDF 的隐写

题目给出一个附件，要求根据附件找到 flag 并上传。

解题思路：

（必定图片下面放着东西），下载好附件，发现是一个 pdf 文件，无法直接移开图片。将它转换为 word 文档，选中照片，直接点复制选择内容，如果照片下面有文本的话就会复制的。之后我们就随便建个文本文档，粘贴，flag 就出现了。



2.解密题

题目给出：

Y3liZXJwZWVjZxtXZWxjb21lX3RvX25ld19Xb3JsZCF9

要求找到 flag 并上传。

解题思路：判断为 base64 编码，通过 base64 解码得到
flag cyberpeace>Welcome_to_new_World!}

第三阶段：线下攻防赛

1. web 服务器提供一个 ping 功能：用户从 web 界面输入目标 IP，提交后，后台会对该 IP 地址进行一次 ping 测试，并返回测试结果。

攻击思路：如果在设计 web 界面 ping 功能时，没有做严格的安全控制，则可能会导致攻击者通过该接口提交“意想不到”的命令，从而让后台进行执行，从而控制整个后台服务器。

直接在 ping 执行栏中输入

127.0.0.1 & cat /key

就可以获取目标主机里面的 key 值，攻击成功，获得积分。

附件 3

第二届广东大学生网络安全攻防大赛报名表

学校名称							
通讯地址							
团队名称							
第一指导老师		联系电话				性别	
第二指导老师		联系电话				性别	
团队 成员	姓 名	所学专业	年 级	性 别	队长/ 成员	联系电话	微信号
指导老师 意见		年 月 日					
所在学校 团委意见		年 月 日					

注：指导老师最多填报 2 人；学生团队指定 1 人为队长。