中国交通运输协会
中国交通通信信息中心 文
交通运输部管理干部学院 件
中国交通报社有限公司

中交协秘字〔2022〕号

关于举办2022年第一届交通运输行业网络安全大赛的通知

各相关单位：

为了深入学习贯彻《网络安全法》、《“十四五”现代综合交通运输体系发展规划》、《交通运输部关于进一步加强交通运输安全生产体系建设的意见》等有关文件要求，落实交通运输行业信息化发展战略，推进交通运输行业信息安全保障体系建设，服务新型网络基础设施建设，推动制造强国和网络强国建设，并大力提升各企业“智慧交通”建设工作中的网络安全防护能力，中国交通运输协会、中国交通通信信息中心、中国交通报社有限公司、交通运输部管理干部学院决定联合主办2022年第一届交通运输行业网络安全大赛。

大赛以交通行业网络安全为方向，围绕车联网、智慧交通、数据安全等行业信息新兴技术开展网络安全大赛，赛程

分为初赛和决赛两个阶段，参赛方式分为通用赛（个人赛、团体赛）、专场赛，本次大赛旨在挖掘和培养交通运输企业网络安全人才，加快企业网络安全人才队伍建设。具体内容通知如下：

一、组织机构

主办单位：中国交通运输协会

中国交通通信信息中心

中国交通报社有限公司

交通运输部管理干部学院

承办单位：交通运输信息安全中心

中国交通运输协会信息专业委员会

交通运输行业网络安全攻防训练基地

技术支持单位：北京益安在线科技股份有限公司

二、大赛组委会

大赛组委会由主办单位、承办单位及技术支持单位等领导组成。组委会组织人员负责线下活动区内各项安全工作，建立公安、消防、司法行政、交通、卫生、食品、质检等相关部门协调机制保证活动安全，并制定应急预案，及时处置突发事件。制定相应安全管理的规范、流程和突发事件应急预案，全过程保证筹备和实施工作安全。

设置一名具有2个以上同类大型项目管理经验的人员作为总负责人，并专门组织团队负责策划、技术、后勤保障、

现场会务接待、安全安保、防疫等方面的工作，保证大赛顺利开展。

三、大赛方案

1.时间和地点

大赛初赛时间：6月23日

大赛初赛举办地点：线上

大赛决赛时间：9月

大赛决赛举办地点：线下

2.比赛说明

大赛初赛：为线上方式比赛，分为通用赛（个人赛、团体赛）、专场赛，比赛内容为网络安全知识考核与CTF竞赛。

大赛决赛：包括网络安全CTF竞赛、网络安全渗透靶场赛和交通运输行业专项场景赛。

3.大赛奖项设置

个人赛排名：

一等奖 1名 （个人成绩排名第1）

二等奖 10名（个人成绩排名第2-11）

三等奖 20名（个人成绩排名第12-31）

团队赛排名：

一等奖 1名 （团队成绩排名第1名）

二等奖 5名 （团队成绩排名第2-6名）

三等奖 10名（团队成绩排名第7-16名）

4.参赛对象、范围和要求

大赛参加对象为综合交通全领域，包括交通运输、铁路、民航、邮政领域企事业单位和个人。

初赛个人赛：交通运输行业相关企业单位的在职安全技术人员。

初赛团队赛：交通运输行业相关企业单位可自行组织队伍。

行业系统专场赛和系列赛：可在系统内部举办专场赛和系列赛，仅该系统内部企事业单位可组建队伍参加。

初赛个人赛取得前20%名次的参赛人员参加线下决赛；初赛团队赛每支队伍不超过5人，每个企业单位最多组建5支队伍，在初赛中取得前10%名次的团队参加线下决赛；专场赛比赛在初赛中取得前10%名次的团队参加线下决赛。

5.报名方式

请参赛单位及个人登录https://sec.motmti.cn网站填写报名信息，报名截止日期为2022年6月20日。

本次大赛免报名费，交通、食宿等费用自理，比赛现场所用电脑、设备数据连接线、转换器等均自行准备。

6.技术培训

本次大赛同时提供相关网络安全技术培训，培训内容涵盖网络安全攻防、网络安全运维、云计算安全、车联网安全、

大数据安全等方面内容，各参赛单位可根据本单位自身需求报名参加。

四、疫情防控措施

大赛严格落实疫情防控要求，进行赛前管控，赛场防控，加强人员管理，根据实际情形对大赛进行调整，如遇疫情无法正常举办，由主办方决定延期或者取消举办，同时立即将原因详情及决定结果通知参赛方。

五、报名联系人

交通运输信息安全中心：冯涛，13426417071，010-65293311；兰昱，13501119015。

中国交通运输协会信息专业委员会：田蒴，18600409749；张诗琪，13683209175，010-68004560。

附件：2022年第一届交通运输行业网络安全大赛赛制方案

中国交通运输协会　　中国交通通信信息中心

交通运输部管理干部学院　　中国交通报社有限公司

2022年5月11日

附件：

2022年第一届交通运输行业网络安全大赛

赛制方案

一、大赛形式

本届活动包含网络安全大赛初赛、网络安全大赛决赛、网络安全大赛结果公布会共3个部分。

网络安全大赛初赛：为线上形式竞赛，由通用赛、专场赛、系列赛多种形式组成。

1.通用赛分为个人赛与团体赛线上模式。比赛内容以CTF竞赛为主，并包含部分网络安全知识和安全运维知识竞赛题目，交通运输部下属企事业单位及交通运输部下属企事业单位在职安全技术人员均可报名参加；

2. 行业系统专场赛和系列赛：可在系统内部举办专场赛和系列赛，仅该系统内部企事业单位可组建队伍参加。

网络安全大赛决赛：为线下形式竞赛。比赛内容为CTF竞赛、靶场竞赛以及交通运输沙盘为场景的专项赛，涵盖车联网安全、大数据安全、云计算安全和智慧交通等方向，决赛将安排在统一会场开展。

网络安全大赛结果公布会邀请领导嘉宾现场为获奖队伍与个人进行颁奖。

二、赛制说明

1.初赛赛制说明

①个人赛。比赛形式为线上平台竞赛，采用CTF解题赛的比赛形式进行，CTF模式包括解题赛及解题过程答辩，题目主要包含逆向、信息解密、隐写，以及车载 CAN 总线通信数据分析等。个人赛时长约为0.5天。

②团队赛。比赛形式为线上平台竞赛，比赛以CTF形式为主，并包含网络安全知识和安全技术理论等，考核团队的综合技术实力。题目主要包含漏洞挖掘与利用、Web渗透、文件与图片隐写、安全编程、车辆协议破解等类别，团队赛需要每个成员通力协作，利用知识和各种工具手段进行赛题解答。团队赛时长约为0.5天。

③行业系统专场赛。根据各行业系统的实际情况和需求，量身定制比赛内容，针对行业关注重点，突出行业特色。比赛形式为团队赛，根据行业系统实际情况可选择线上或线下形式比赛。比赛时长约为0.5天。

2.决赛赛制说明

①个人赛。比赛形式为现场竞赛。主要为CTF解题赛的比赛形式进行，题目主要包含逆向、漏洞挖掘与利用、Web渗透、密码、取证、隐写、安全编程等类别，选手通过解题获得相应题目中的Flag，并提交至评分系统以获得相应的分

值，综合考察选手的技术能力、计算能力、工具运用能力和安全知识范围。个人赛时长约为 0.5 天。

②团队赛。团队成员以靶场提供的综合模拟环境为目标，运用技能和工具挖掘服务器漏洞，竞赛主题包括基础安全和行业工控安全等，参赛团队需要充分运用每个成员的特长和技术，合理分配人员和资源，考察队伍的综合技术实力以及团队合作能力。团队赛比赛时长约为 0.5 天。在团队赛过程中，参选者队伍在规定时限内轮流参加场景专项赛对沙盘开展攻击获取分数，沙盘被攻击后将恢复初始状态，确保比赛的公平性。

三、大赛题型说明

1.CTF 比赛。是以综合分析与解密技术相结合的比赛，选手需要仔细观察赛题，利用自身知识和经验，以及使用擅长的工具对赛题进行破解，取得其中的关键信息。例如，赛题可能是一段代码、一个流量数据包，甚至是一张图片，选手需要对数据进行分析，找到其中关键点，或者对表现异常的数据进行变换，最终找到其中隐藏的正确答案。CTF 比赛除了提交正确答案（flag）外，还需要简单记录解题过程（writeup），最终一同提交，裁判将根据两项内容综合判定。同时，比赛为了确保公平并防止作弊，每个选手的题型、解题过程均相同，但最终 flag 字符串不相同，如发现提交了其他选手的 flag 将视为作弊及扣分。

2. 靶场比赛。通过靶场平台，为每支参赛队伍搭建一套贴合行业业务情况的真实环境，环境内分为DMZ、内网、生产等区域，并包含路由器、交换机防火墙等设备，参赛队伍需要综合利用自身知识和技术技巧，利用各项工具开展漏洞挖掘、渗透等攻击行动，对环境内的各种设备开展攻击，取得控制权并逐步深入推进。整体比赛环境与真实环境复杂度十分相似，参赛队伍可选择不同路线开展攻击，需要充发挥每一位队员擅长的技术领域，合理分配资源与任务，考验团队合作能力。靶场平台将会记录每一位选手的攻击与取得成果，最终进行综合评分。

3. 交通运输行业场景专项赛。在比赛场地搭建行业沙盘，配合系统靶场，布置典型场景例如车辆信息、交通信号、路况采集等，并配置后台控制系统，比赛时间内，队伍可以使用各种方式自由渗透及挖掘系统漏洞，找到入侵系统路径并成功控制系统，当控制系统被攻陷后，参赛者可通过系统操控沙盘做出响应，例如声光、车辆或信号灯的动作等，具备非常好的现场展示效果。专项场景赛根据参赛队伍攻击成功的系统设备进行评分。

四、大赛评选与评分说明

1. 评选工作机制

大赛成立评委工作组，比赛分数由电脑自动生成，由大赛评委工作组成员完成统计、公布，大赛评委工作组的技术人员及相关专家对大赛进行全程管理、监督及指导。

2.评分说明

网络安全大赛各环节均是计分制，按照题目难度设置不同分值，网络安全大赛结束后将在现场进行各项成绩统计，按个人、团队成绩排名，并邀请领导嘉宾现场为获奖人员与队伍颁发奖杯、荣誉证书。

个人赛初赛：CTF 解题赛，共 12 道题，选手答对各赛题获得对应的分值，总分为 800 分。题目主要包含逆向、信息解密、隐写，以及车载 CAN 总线通信数据分析等，为防止作弊，CTF 解题模式采取动态 flag 模式，即各团队的所有题目均拥有唯一 flag 值，如果提交其参赛人员的 flag 会被扣除当前题目总分值的 50%。

团队赛初赛：CTF 解题赛，12 道 CTF 总共 1200 分，包含网络安全知识和安全技术理论等选择题 100 道总共 100 分考核团队的综合技术实力。题目主要包含漏洞挖掘与利用、Web 渗透、文件与图片隐写、安全编程、车辆协议破解等类别，团队初赛总计 1300 分为防止作弊，CTF 解题模式采取动态 flag 模式，即各团队的所有题目均拥有唯一 flag 值，如果提交其他团队的 flag 会被扣除当前题目总分值的 50%。

行业系统专场赛初赛：根据各行业系统的实际情况和需求，量身定制比赛内容，针对行业关注重点，突出行业特色。

个人决赛赛：比赛形式为现场竞赛。主要为 CTF 解题赛的比赛形式进行，12 道 CTF 总共 1200 分题目主要包含逆向、漏洞挖掘与利用、Web 渗透、密码、取证、隐写、安全编程等类别，选手通过解题获得相应题目中的 Flag，并提交至评分系统以获得相应的分值，综合考察选手的技术能力、计算能力、工具运用能力和安全知识范围。

团队赛决赛：靶场模式，环境内分为 DMZ、内网、生产等区域，并包含路由器、交换机防火墙等设备，参赛队伍需要综合利用自身知识和技术技巧，利用各项工具开展漏洞挖掘、渗透等攻击行动，对环境内的各种设备开展攻击， 取得控制权并逐步深入推进共计 6 个靶场里含多个动态 FLAG，总分共计 1200 分。

团队赛决赛：交通运输行业场景专项赛模式，在比赛场地搭建行业沙盘，配合系统靶场，布置典型场景例如车辆信息、交通信号、路况采集等，并配置后台控制系统，比赛时间内，队伍可以使用各种方式自由渗透及挖掘系统漏洞，找到入侵系统路径并成功控制系统，当控制系统被攻陷后，参赛者可通过系统操控沙盘做出响应，例如声光、车辆或信号灯的动作等，总分共计 800 分。