附件

2023年四川省网络与信息安全技能大赛

技术文件

目录

一、大赛概述

为鼓励从业人员不断学习和改进自身技能，以适应快速变化的网络安全环境，举办本次技能大赛。大赛提供专业化的比赛平台，将从政策法规标准和网络攻防、漏洞挖掘与利用、Web 渗透测试、数据取证、工控安全和信创安全等方面，围绕信息系统可能存在的网络安全事件进行的事前检测与防护、事中应急与防御、事后取证与溯源等技术要点展开，贴近实际的案例和应用场景，全方位考核从业职工的网络安全综合能力。

通过大赛，相关企事业单位人员能够接触到最新的技术和行业趋势，了解各种攻防策略和解决方案，增进相互间的技术交流，进一步提高信息安全从业人员的专业知识与实践技能水平，更好地激励企业加强自身安全队伍的培养，切实提升自己安全防护综合能力。推动行业人才的培养和发展，为网络安全工作持续有效的开展起到积极的促进作用。

二、大赛形式及内容

本次大赛由线上初赛和线下决赛两部分组成。分为个人赛和团队赛，团队赛中每支队伍由 3 名选手组成（每人只能参加一支队伍）。

线上初赛分为个人赛和团队赛，采用“综合理论赛”与“夺旗解题赛”的方式进行。

线下决赛分为个人赛“夺旗解题赛”，团队“AWD 攻防赛”，由线上初赛中入围的选手和团队进行参赛。

初赛成绩不作为决赛排名的参考依据。

赛事阶段	参赛形式	赛制	
初赛	个人	综合理论赛	夺旗解题赛
	团队		夺旗解题赛
决赛	个人	夺旗解题赛	
	团队	AWD 攻防赛	

1、初赛

初赛地址、账号等具体信息将在赛前 3 个工作日内通过报名时预留的联系方式以短信方式通知到每位参赛选手。

为保障参赛顺利，请选手在 2023 年 10 月 10 日 9：00-18：00 期间登录大赛账号，提前熟悉平台。

1.1、综合理论赛

本赛项采用线上模式进行。

参赛人员：所有报名参与个人赛和团队赛的人员。

（1）综合理论赛大赛内容。

考试时间为 1 小时，总分 300 分。考点主要包括：法律法规、政策标准和网络安全技术知识等。

题目总数 100 道题，其中单选题 60 道，分值为 2 分/道；不定项选择题 20 道，分值为 6 分/道；判断题 20 道，分值为 3 分/道。

1.2、夺旗赛

本赛项采用线上模式进行。分为“个人夺旗赛”和“团队夺旗赛”。

（1）积分方式

根据每道题目难度不同，将每道题分数设置为 100、200、

300 分。前三名答题成功的参赛选手可额外获得本题分值的 15%、10%、5%的奖励分。参赛选手将按照当前积分高低进行排名，如果出现选手同类分值相同的情况，根据答题时间做优先级排名。

（2）注意事项：参赛选手须在比赛结束后 4 小时内将完整解题报告（writeup，PDF 格式）上传至大赛平台，未提交解题报告的，裁判组将默认该题成绩无效，如有以下情形将进行扣分处理:

①不同参赛选手提供了相同 writeup，扣除双方本题分数;

②writeup 不完整，或过于简洁，扣除本题分数。

1.2.1、个人夺旗赛

参赛人员：报名参与个人赛人员。

（1）个人夺旗赛大赛内容

考试时间为 3 小时,共 10 道题,总分 1600 分(不含奖励分)。

题目设置:普通难度 6 题(每题 100 分)、中等难度 2 题(200 分）、较高难度 2 题（每题 300 分）

考点主要包括：Web 安全、Crypto 密码学、Reverse 逆向工程、Pwn 二进制漏洞利用、Misc 安全杂项等。参赛选手结合题目环境以及题目描述，解决网络安全技术问题，利用安全工具、安全漏洞等手段寻找考题的 flag 值,参赛选手将获取到的 flag 提交至大赛平台。

（2）个人夺旗赛成绩

成绩占比：综合理论赛占个人初赛成绩 30%，个人夺旗赛成绩占个人初赛成绩 70%。

成绩计算方式：个人总成绩=本人理论成绩/本场理论成绩

最高分*30+本人夺旗解题赛成绩/本场个人夺旗解题赛最高分*70

注:若个人总成绩相同，则按夺旗解题赛成绩排名。

1.2.2、团队夺旗赛

参赛人员：报名参与团队赛的所有人员。

（1）团队夺旗赛大赛内容

考试时间为 5 小时，共 15 道题，总分 2500 分（不含奖励分）。

题目设置:普通难度 8 题(每题 100 分)、中等难度 4 题(200 分）、较高难度 3 题（每题 300 分）

考点主要包括：Web 安全、Crypto 密码学、Reverse 逆向工程、Pwn 二进制漏洞利用、Misc 安全杂项等。参赛选手结合题目环境以及题目描述，解决网络安全技术问题，利用安全工具、安全漏洞等手段寻找考题的 flag 值,参赛选手将获取到的 flag 提交至大赛平台。

（2）团体夺旗赛成绩

成绩占比：团队综合理论赛占团体赛成绩 20%，团队夺旗赛成绩团体赛成绩 80%。

成绩计算方式：团队总成绩=本队参赛成员理论成绩总分/本场团队理论成绩总分最高分*20+本队夺旗解题赛成绩/本场团队夺旗解题赛最高分*80

注:①参加团队赛所有成员都必须参加“综合理论赛”。

②若团队总成绩相同，则按夺旗解题赛成绩排名。

2、决赛

2.1、个人赛决赛

个人赛决赛采用线下集中比赛模式，以夺旗解题赛方式进行，决赛总时长 4 小时。

参赛人员：个人赛初赛排名前 60 名的选手。

（1）大赛内容

个人赛决赛共 10 道题，其中 Web 安全题目 3 道，Crypto 密码学题目 1 道，Reverse 逆向题目 1 道，Pwn 题目 2 道，Misc 杂项题目 2 道，IOT 题目 1 道。

题目设置为普通难度题目 4 题，中等难度题目 3 题，较高难度题目 3 题。

比赛内容主要包括：漏洞挖掘、渗透测试、逆向分析、代码分析、加密解密、日志分析、数据分析、移动互联网应用安全等技术等。IOT 题目涵盖固件安全等。工控考点包括工程文件分析及相关逆向能力等。

（2）计分方式

个人赛决赛 CTF 每道题的初始分值为 500 分，每道题目的分值都会随着解出此题的人数增加而减少，参赛选手已获得的积分也会随着已解出题的解题人数增加而动态变化，直到已解出题的题目分值降到最低分时（最低分为 200 分）不再变动。参赛选手按照比赛结束时积分高低进行排名。当积分相同时，先达到该积分的（用时最短）排名靠前。

2.2、团体赛决赛

团体赛决赛采用线下集中比赛模式，以 AWD 攻防赛方式进行，

总时长 3 小时。

参赛队伍： 团队赛初赛排名前 20 名的队伍

（1）大赛内容

AWD攻防赛模式为每支参赛队伍提供多个网络场景(靶机),各参赛队伍之间的网络场景互通,在限定网络内互相进行攻击和防守。靶机中部署有若干漏洞环境，参赛队员可利用管理员提供的登录信息（用户名、口令、IP 地址）登录靶机进行安全加固。在比赛过程中,参赛队伍利用对方服务器上的任意漏洞成功获取其服务器权限后，运行指定命令得到 Flag，然后将得到的 Flag 在答题界面提交得分。同时，对方因为未修复漏洞被攻击成功而扣分。在比赛过程中，所有参赛队伍均应保持自己的靶机服务及业务运行正常、没有违规操作。大赛平台会监控所有靶机的服务及业务运行情况,并对靶机运行异常或存在违规操作的队伍作出扣除 30 分的处罚。

（2）计分方式

AWD 攻防赛采用轮次计分方式，10 分钟为一轮次。在同一轮次内，一支队伍只可提交另一支队伍 1 次 Flag，即 A 队在某轮次内只能从 B 队获取一次分数，在下一轮次开始后，A 队可重新从 B 队获取分数。

计分方式采用“零和”计分模式:

零和积分模式: 每支参赛队伍均有固定的初始分数。比赛开始后即可对其他队伍的靶机发起攻击并维护己方靶机。每轮次内，如己方靶机被攻陷（靶机被其他队伍获取权限后提交了 Flag），该靶机将被扣除 30 分，并在本轮次结束后作为奖励平均分配给

本轮次内所有成功攻陷此靶机的队伍。

同时，在比赛过程中所有队伍均应保持所有靶机提供的服务运行正常。若大赛平台监控到某队伍靶机服务运行异常（包括业务异常或其它违规操作），则会作出扣除 30 分的处罚，并将该分数作为奖励平均分配给本轮次内此靶机保持服务正常的所有队伍。

每支参赛队伍设置有最低分，当队伍积分达到最低分时，不再进行扣分。

三、大赛大纲

本次比赛有三种赛制类型，分别是综合理论赛、夺旗解题赛、AWD 攻防赛。

1、综合理论赛

1.1 赛制说明

综合理论赛采用单项选择，不定项选择和判断三种类型组合而成。综合理论赛全面考察参赛选手个人的综合基础知识，以及选手对国家、行业、安全标准的政策、法律法规的理解。

1.2 比赛范围

题目类型	方向	考点
理论题	移动安全	密码学——基础理论与应用
	接入安全	中华人民共和国个人信息保护法
	主机安全	中华人民共和国数据安全法
	网络安全	中华人民共和国密码法
	办公安全	中华人民共和国网络安全法
	数据库安全	中华人民共和国电子商务法

	云安全	中华人民共和国电子签名法
	密码学	关键信息基础设施安全保护条例
	法律法规	中华人民共和国计算机软件保护条例
	安全防护	互联网信息服务管理办法
	安全运维	计算机信息网络国际联网安全管理保护办法 信息系统安全等级保护实施指南

1、法律法规

了解相关网络安全防护范围、管理主体、责任主体、同步要求、分级备案要求、符合性评测要求、风险评估要求、应急演练要求等内容。

2、政策文件

了解电信网络安全防护工作总体思路、基本原则、主要任务、实施及监督检查要求、安全服务机构管理等政策文件；了解电信网络等级保护工作的目的、原则、意义、要求、思路、实施内容、流程等政策内容；熟悉电信网络等级保护定级范围、评审要求、备案等政策要求，熟知电信网络单元安全防护定级方法、定级对象命名规则、定级报告内容、定级备案相关信息等。深入了解运营商行业信息安全管理体系认证相关工作的目的、意义以及要求。熟悉应用网络单元安全防护检测评分方法等内容。

3、网络安全防护相关标准

了解安全防护定义、目标、基本原则、体系及各部分工作内容等内容。熟悉安全等级划分、定级对象划分、定级方法及要素、等级保护原则和实施过程等相关标准；了解安全风险评估要素及关系、工作形式、遵循原则、实施流程、在不同生命周期中的要

求和实施要点等标准；了解灾难备份等级划分、灾难备份原则、灾难备份资源要素、实施过程、灾难恢复预案要求等防护标准。深入了解安全管理制度、安全管理机构、人员安全管理、安全建设管理、安全运维管理等内容。

4、操作系统安全检测与防护

了解操作系统（Windows、Linux、Unix 等）的常规安全防护技术；能熟练利用系统日志、应用程序日志等溯源攻击途径；掌握系统账号、文件系统、网络参数、服务、日志审计等项目的安全检测与安全加固方法。

5、数据库安全检测与防护

了解数据库（Mssql、Mysql、Oracle、MongoDB）的库表管理、权限控制等数据库管理方式；熟悉数据库入侵防御、访问身份认证、数据加密等其他安全措施；深入了解数据库的客户端程序管理、应用系统访问、客户端访问控制、重要操作审计以及数据备份。

6、网络攻击与防护

熟悉网络层攻击原理及防护方法，能运用相关工具及技术手段发现并阻断网络层攻击、验证无线网络 WEP、WPA 和 WPA2 的密码强度。其中常见网络层攻击包括：中间人攻击、DHCP 攻击、DDOS 攻击、无线 DDOS 攻击、无线 WAPjack 攻击等；熟悉常见网络安全设备的功能及使用方法，包括：防火墙（含 Web 应用防火墙）、入侵检测系统、抗拒绝服务攻击系统、网页防篡改系统、漏洞扫描系统等。

7、Web 应用安全

了解常见 Web 环境（ASPX、PHP、JSP）的搭建方法以及安全配置方法；熟悉中间件和 Web 应用的安全检测与防护方法。漏洞包括：权限绕过、弱口令、注入、跨站、文件包含、文件上传、命令执行、任意文件读取和下载等。

8、渗透测试技术

掌握常规的渗透测试技术；熟悉使用各种常见渗透测试工具。渗透测试技术包括：扫描探测、信息收集、暴力破解、常规漏洞利用、Web 权限获取、提权、溢出攻击等。

9、应急响应与数据恢复

掌握应急响应和数据恢复的流程和相关技术，包括：入侵取证分析、反取证技术、日志审计分析、日志删除恢复、文件删除恢复、硬盘格式化数据恢复等。

10、开发安全

了解常见编程环境（C、JAVA、PHP、JSP）的构建以及语言的编写；熟悉缓冲区溢出、拒绝服务等编码防御技术；掌握代码审计和代码加固技术，避免出现常见安全漏洞。常见漏洞至少包括：缓冲区溢出、拒绝服务、远程命令执行、注入、跨站。

11、恶意代码与逆向

熟悉操作系统中恶意代码的识别方法及防护措施，能运用相关工具及技术手段发现、隔离、清除常见恶意代码，其中常见恶意代码包括：注册表级后门、Rootkit、远程控制木马、键盘记录木马、网页木马、Webshell 等，并能对常见恶意代码进行逆向分析及源定位。

12、移动应用安全

了解移动智能终端操作系统、移动应用软件的常规安全漏洞检测和防护技术；熟悉移动互联网恶意程序相关监测与处置机制；掌握移动应用的逆向分析和代码审计技术、移动应用的安全防护方法等。

2、夺旗解题赛

2.1 赛制说明

在解题模式 CTF 赛制中，参赛选手通过互联网参与，参赛选手通过与在线环境交互或文件离线分析，解决网络安全技术挑战获取相应分值，根据总分和时间来进行排名。

2.2 比赛范围

题目类型主要包含 Web 安全、Crypto 密码学、Reverse 逆向工程、Pwn 二进制漏洞利用、Misc 安全杂项、工控协议以及信创安全这七个类别。

类型	CTF 知识体系大纲
Web 安全	信息泄露、代码审计 Cookie 伪造、社会工程、命令注入、XSS 盲打、端口扫描、x-forwarded-for 绕过限制、orderby 注入、SQL 注入、搜索型 SQL 注入、SSRF 漏洞、CSRF 漏洞、PHP 反序列化、WAF 绕过漏洞、暴力破解、目录遍历、文件包含、任意代码执行、文件上传漏洞、任意文件下载、弱口令、隐藏字段、robots.txt、j2ee 框架漏洞、Strtus2 框架漏洞、PHP 反序列化、TOMCAT 漏洞、权限漏洞、业务逻辑支付漏洞、旁注漏洞、JS 前端校验等。
Crypto 密码学	DES、奇偶校验（汉明码）、算法、算法编程、文件格

	式、jother、移位密码、频率分析、维吉尼亚解密、Windows 密码、Rabin 加密算法、乐谱隐藏、替换密码、频率攻击、base64 解密、md5 破解、栅栏密码、猪圈密码、RAR 破解、四方密码、中文电码、RSA 共模攻击、维吉尼亚、频率攻击等。
Reverse 逆向工程	EXE 程序逆向、APK 逆向、算法分析、固件逆向、注册机逆向、逆向算法、JAVA 逆向、JAVA 编程、脱壳、IDA 分析、脱壳技术等。
Pwn 二进制漏洞利用	Linux 本地、Windows 本地、远程溢出，二进制文件分析、溢出代码编写、IDA 分析、NC 反弹技术等。
Misc 安全杂项	图片隐写、LSB 水印算法隐藏、二维码技术、音频分析、摩斯电码、ZIP 暴力破解、数据分析、网络分析、二进制取证分析、网络抓包分析、Base64 解密、APK 逆向分析、APK 木马分析、Webshell 查杀、编程、社会工程、编程、应急响应、文件头修改、文件头修复、图片分离、pngcheck、摩斯电码等。

3、 AWD 攻防赛

3.1 赛制说明

AWD 攻防赛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。

在攻防模式中，初始时刻，所有参赛队伍拥有相同的系统环境(包含若干服务，可能位于不同的机器上)，常称为 gamebox，

参赛队伍挖掘网络服务漏洞并攻击对手服务获取 flag 来得分，修补自身服务漏洞进行防御从而防止扣分。

3.2 比赛范围

题目类型	方向
WEB-AWD	SQL 注入
	任意文件操作
	命令执行
	反序列号
	代码审计
PWN-AWD	栈溢出
	格式化字符串
	堆利用