附件 2：

2022 年川渝网络与信息安全职业技能竞赛

技术文件

2022 年 8 月

目录

一、竞赛情况

鉴于参赛选手日常工作的主要职责是保障信息系统安全稳定运行，大赛将从政策法规和标准、网络安全风险评估、物联网安全、应急响应技术、信创等方面，围绕信息系统的事前检测与防护、事中应急与防御、事后取证与溯源等技术要点展开，全方位考核从业职工的网络安全综合能力。

二、竞赛形式及内容

本次竞赛分为个人赛和团体赛两个赛程，分设初赛、决赛两个赛段。初赛采用线上比赛模式，决赛采用线下集中模式。

初赛地址、账号等具体信息将在报名截止后 3 个工作日内通过报名时预留的联系方式分别以短信、邮件的方式通知到个人。

（一）个人赛

1、个人赛初赛

本赛项采用线上“理论+CTF”的模式进行，总时长 6 小时，前 1 小时进行理论竞赛，后 5 小时进行 CTF 竞赛。

参赛人员：所有报名参赛的人员

（1）理论赛竞赛内容

考试时间为 1 小时，总分 100 分，按照 30%计算入初赛成绩。

考点主要包括：政策法规标准等法律法规和网络安全技术知识点。题目总数 70 道题，其中单选题 30 道，分值为 1 分/道；多选题 30 道，分值为 2 分/道，判断题 10 道，分值为 1 分/道。

（2）CTF 夺旗赛竞赛内容

考试时间为 5 小时，共 15 道题，按 70%计算入初赛成绩。

考点主要包括：Web 安全、Crypto 密码学、Misc 安全杂项、Reverse 逆向工程、Pwn 溢出等。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 提交至竞赛平台。

（3）计分方式

每道题的基础分数为 800 分，设置递减系数为 0.01，每道题得分将会随着解出人数的增加而减少，当得分减少到小于等于 100 分时，后续解答正确的选手分值按照 100 分计。【计算公式：参赛选手得分=题目基础分值-题目基础分值*（当前名次-1）*0.01】（当前名次为选手提交有效答案时该题的解题顺序排名）。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。

注意：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）上传至竞赛平台，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；

② writeup 不完整，或过于简洁。

2、个人赛决赛

个人赛决赛采用线下集中比赛模式，以 CTF 方式进行，决赛时长 4 小时。

决赛地点：成都信息工程大学体育馆（四川省成都市西南航

空港经济开发区学府路一段 24 号)。

参赛人员：个人赛初赛排名前 90 名的选手

（1）竞赛内容

个人赛决赛共 10 道题，其中杂项 2 道，Web 安全 2 道，密码学 1 道，逆向 1 道，PWN 2 道，IOT 题 2 道。

比赛内容主要包括：漏洞挖掘、渗透测试、逆向分析、代码分析、脱壳技术、漏洞修复、加密解密、日志分析、安全取证、无线安全、编程开发、WEB 安全防护、数据分析、移动互联网应用安全、物联网安全、数据安全、个人隐私保护、新技术新应用及工作生活相关安全问题等技术等。IOT 题目涵盖硬件安全、固件安全、软件无线电、嵌入式 Web&PWN、蓝牙安全等。工控考点包括 S7Comm 流量分析、工程文件分析及相关逆向能力，软件组态、梯形图逻辑等。

（2）计分方式

个人赛决赛 CTF 每道题的基础分为 1000 分，采用动态积分模式计算，即题目基础分值*加权系数,其中加权系数=1-当前名次/队伍数量（当前名次为选手提交有效答案时该题的解题顺序排名），或者加权系数=动态计分阈值。如果系数大于或者等于动态计分阈值，则按照当前的系数计算，如果小于动态计分阈值，则系数按照动态计分阈值计算。第一个队伍得赛题分数满分（系统自动设定），越靠后解出的队伍得分越低，直至设置的最低阈值。

（二）团队赛

1、团队赛初赛

本赛项采用线上 CTF 的模式进行，总时长 7 小时。

参赛队伍：所有报名参赛且组队成功的团队

（1）竞赛内容

团队赛初赛共 15 道题，考点主要包括：Web 安全、Crypto 密码学、Misc 安全杂项、Reverse 逆向工程、Pwn 溢出等。

（2）计分方式

队员计分方式与个人赛初赛 CTF 夺旗赛一致，团队成绩按三名队员成绩总和排名。

2、团队赛决赛

决赛采用线下集中比赛模式，以 AWD 攻防赛方式进行，共 3 个小时。

决赛地点：成都信息工程大学体育馆（四川省成都市西南航空港经济开发区学府路一段 24 号）。

参赛队伍：团队赛初赛排名前 30 名的队伍

（1）竞赛内容

团队赛决赛内容涉及 WEB 安全与加固、PWN 类，各参赛队伍之间的网络场景互通，在限定网络内进行互相攻击和防守。参赛选手每队分配一套相同的网络环境,有 2 台服务器(Linux 主机，靶机）需要维护，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。每队分配的管理用户非 root，为低权限用户。参赛选手需在规定时间内充分挖掘漏洞并利用，提交其他选手的旗标得分，同时通过修补自身防守机的漏洞进行防御来避免失分。

（2）计分方式

AWD 攻防赛每队基础分为 70000 分，得分不设置上限。比赛用时 180 分钟（3 个小时），其中加固 30 分钟，混战 150 分钟。

（1）每队基础分值 70000 分，漏洞被攻击者成功利用，守方掉分、攻击方得分（得失分相当）；

（2）每个题目各有 1 个 flag（分别位于系统根目录），攻击开始后 flag 每 20 分钟变一次，分值不变，flag 分值 100 分；

（3）得分相同者，先提交者排名在先；

（4）对攻开始后（开赛 30 分钟后可以开始攻击），同时裁判不定时进行检测服务，如果裁判检测到任何一支队伍服务宕机（端口、web 标志文件无法访问、系统功能不正常、使用通用 WAF 等），无论任何原因服务器所属队伍扣分，每次扣 500 分/点；

（5）每队服务器漏洞环境完全一致；

（6）如果对方没有修复漏洞，每 20 分钟还可以提交对方变化后的 flag 进行得分；

（7）团队赛成绩算法：参赛队伍团队赛最终得分= 攻防对抗竞赛系统上所显示的参赛队伍得分。

（8）每个队伍在竞赛中每台服务器主机仅可申请两次重置主机，每个主机重置一次需要扣除对应团队分 5000 分（需获取现场裁判许可，且参赛队伍所有成员签字确认）。

三、决赛前培训

参培人员：进入决赛的选手及团队。

方式：采用腾讯会议线上授课模式进行，竞赛组委会根据入围决赛名单以邮件形式通知参训选手具体时间、培训会议地址及登陆口令，培训当天，竞赛组委会核实培训选手身份后开始培训。

培训内容：决赛平台介绍、例题讲解、竞赛规则及注意事项、互动问答等（具体内容另行通知）。

四、应急响应及灾备方案

（一）数据备份

平台共部署两台数据库，一台负责平台数据写操作；一台负责主动读的操作。利用主从数据库来实现读写分离，从而减轻主数据库压力，减少平台崩溃风险。通过数据库服务监控服务来保证数据库运行正常。平台数据为同步复制，每隔 5 分钟对数据库进行备份，并将备份数据保留在服务器上。

（二）灾难恢复

竞赛平台软件使用微服务架构开发，容器化部署的方式，可以便捷的横向扩展。如遇节点故障，可在 5 分钟内快速重新部属额外节点替换故障节点。

（三）比赛稳定性保证

比赛期间配备专门的平台运维团队，提供技术咨询，以保障平台的稳定运行。

（四）决赛保障

现场会配备发电设施，应对停电的突发状况。同时安排专业人员进行紧急维修，期间不会中断竞赛。服务器交换机接入双路电，服务器或核心交换机接入双电源。

决赛前进行模拟演练，确保交换机正常运行现场会配备备用交换机。

五、竞赛需知

（一）疫情安全保障

高风险地区的选手不得参加线下比赛。所有人员须持有“健康码、行程码”绿码以及 24 小时内纸质核酸检测阴性证明，接受现场体温检测，符合防疫要求后方可进入活动地点。体温在 37.3 摄氏度及以上人员、发热和咳嗽等症状人员不得进入，同时立即报告并按要求安排就医。

竞赛组委会将根据当地政府发布的疫情防控政策对决赛期间的防疫要求进行相应调整，并在报名网页发布，请提前关注。

（二）竞赛注意事项

1、参赛选手自行准备电脑参加本次竞赛，需提前准备好各类工具和软件。

2、初赛理论赛，建议参赛选手全程采用 chrome、firefox 浏览器进行访问，采用其他浏览器，可能造成平台无法访问，答题异常等情况。

3、决赛现场仅提供有线接入方式，如有必要，参赛选手需

自带 RJ45 网线转接器。

4、决赛竞赛期间参赛选手凭参赛证入场。

（三）竞赛规则

1、禁止参赛选手之间互相共享登陆账号，或将账号共享给其他无关人员。

2、禁止参赛选手共享 flag、hint、解题思路等任何比赛相关信息。

3、禁止攻击比赛平台，如果发现平台漏洞，请立刻向竞赛组委会报告。

4、禁止向比赛平台发送大量流量或使用与比赛题目无关的高速扫描器。

5、禁止对提交的 flag 进行爆破。

6、禁止对现场网络环境进行破坏。

7、禁止个人赛参赛选手合作解题。

8、禁止参赛选手在决赛期间使用任何方式连入互联网。

9、个人赛决赛及团体赛期间所有参赛选手将被分配到不同的环境，禁止访问他人环境。

10、团体赛决赛期间所有参赛选手加固时不能使用 WAF 等工具阻断流量，如发现使用通用 WAF 等阻断流量者每次扣 500 分。

11、参赛选手如有任何违反本注意事项禁止的行为及其他经裁判组判定的违规行为，裁判将会视情况予以警告，扣分或者取消比赛资格，并全场公告。

12、比赛过程中，参赛选手请遵守工作人员指示，尊重裁判

裁决。

13、竞赛组委会拥有对赛题、规则等一切事项的最终解释权。

14、竞赛组委会视疫情防控、比赛具体进度及现场变化，有权调整相关竞赛安排。

六、竞赛大纲

（一）理论题大纲

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。参考法规：《中华人民共和国国家安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国密码法》《中华人民共和国电子签名法》《网络安全等级保护条例》《关键信息基础设施安全保护条例》。

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。参考文件：《通信网络安全防护管理办法》《关于加强网络安全学科建设和人才

培养的意见》《工业和信息化部关于加强电信和互联网行业网络安全工作的指导意见》《工业控制系统信息安全行动计划（2018-2020 年)》《网络与信息安全管理员（网络安全管理员）国家职业技能标准》高级（三级)。

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；了解安全风险评估工作的国际标准名称（ISO/IEC TR 13335、ISO/IEC 17799、ISO/IEC 27001 等)；了解国内由公安部组织制定并发布的《信息系统安全等级保护定级指南》、《信息系统安全等级保护实施指南》等国家标准总体情况。

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。

13、新技术应用

了解云计算和大数据的基本概念及特征;熟悉云计算和大数据技术带来的安全问题；掌握如何使用大数据分析安全事件以及大数据平台本身安全漏洞和隐患的发现。内容包括：虚拟机安全、应用程序安全、数据安全；

了解物联网的基本概念及工作协议和频段,掌握 ID/IC 卡的安全漏洞检测和发现，掌握智能卡的常见加解密算法、多级秘钥

离散机制、随机挑战响应机制和静态/动态数据验证。

（二）CTF 知识大纲

包括 Web 安全、密码学、逆向工程和杂项等，知识技能大纲至少包含如下内容：

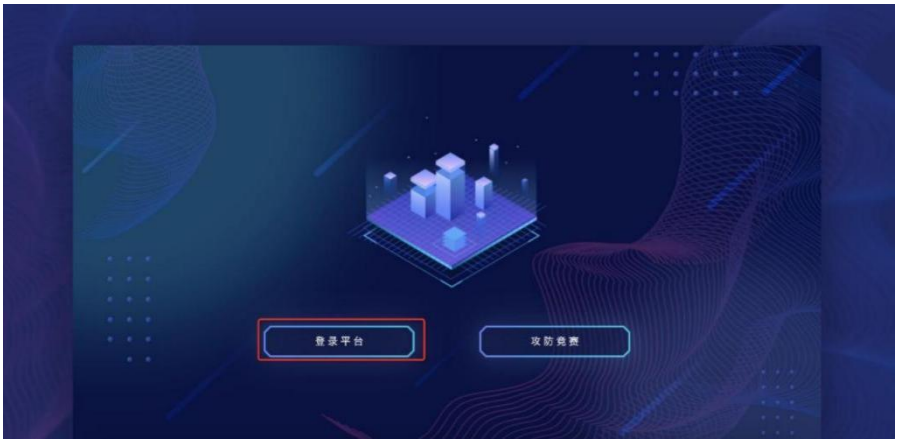
类型	CTF 知识体系大纲
Web 安全	信息泄露、代码审计 Cookie 伪造、社会工程、命令注入、XSS 盲打、端口扫描、x-forwarded-for 绕过限制、orderby 注入、SQL 注入、搜索型 SQL 注入、SSRF 漏洞、CSRF 漏洞、PHP 反序列化、WAF 绕过漏洞、暴力破解、目录遍历、文件包含、任意代码执行、文件上传漏洞、任意文件下载、弱口令、隐藏字段、robots.txt、j2ee 框架漏洞、Strtus2 框架漏洞、PHP 反序列化、TOMCAT 漏洞、权限漏洞、业务逻辑支付漏洞、旁注漏洞、JS 前端校验等。
Crypto 密码学	DES、奇偶校验（汉明码）、算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

七、竞赛平台操作手册

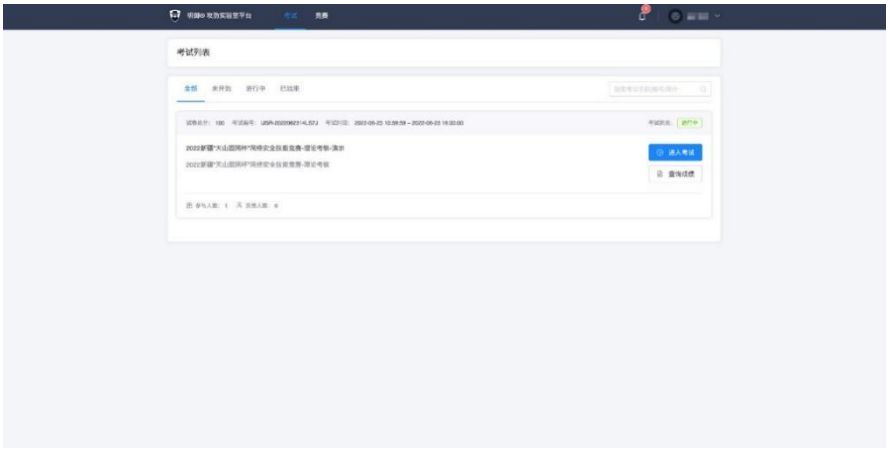
（一）初赛平台

进入网址后点击登录平台，输入账号密码即可进入平台。



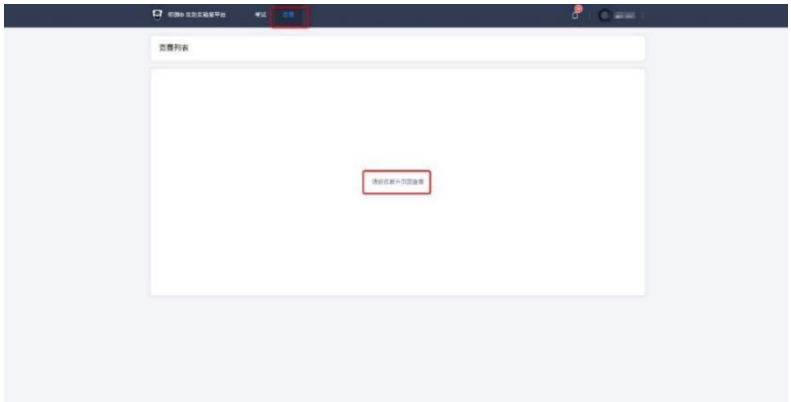
1.理论考试

登录后即为理论考试界面，选择进入考试即可进行答题。



2.CTF 初赛实操考核

点击首页上方的竞赛，平台会打开新页面出现竞赛列表，选择进入 CTF 实操。



进入竞赛后先选择阶段，再点击赛题分组，选择题号后，右侧会出现赛题详情，根据赛题附件或者相关靶机进行解题，获取 flag。获取 flag 后请在赛题详情下方提交 flag。

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）上传至竞赛平台（所有题目的解题报告放到一个 pdf 里），报告须包含解题的关键步骤和 flag 截图，提交的入口如下图“5.提交解题报告”所示。

（二）CTF 决赛平台

1）使用 FireFox 浏览器最新版（请自行准备）访问信息表中提供的平台地址进行登录，使用本次比赛下发的用户名密码进行登录，如存在登录无响应内容，请举手示意裁判；

2）登录成功后，点击右上角从左至右第一个图标，选择“竞技靶场”进入所在 CTF 答题考场；

3）此处是 CTF 答题考场，左边侧栏显示题目类型，点击“类型名称-题目标题”按钮，即可定位至相关题目处；

4）在 flag 输入框中按照题目要求格式输入 flag，点击“提交”即可进行 flag 提交；

5）附件题目点击“附件标题”即可进行附件下载；

6）Web 题目中复制题目描述中“题目地址”或“备用”至新窗口即可进行题目访问；

7、右上角显示竞赛倒计时，请各位选手注意时间节点。

（三）AWD 决赛平台

1、使用 FireFox 浏览器最新版（请自行准备）访问信息表中提供的平台地址进行登录，使用本次比赛下发的用户名密码进行登录，如存在登录无响应内容，请举手示意裁判；

2、登录成功后，点击右上角从左至右第一个图标，选择“竞技靶场”进入所在 AWD 答题考场；

3、此处是 AWD 答题考场，可看到自己的 AWD 防守靶机，以及提供的相关用户和密码。

4、在 flag 输入框中按照题目要求格式输入 flag，点击“提交”即可进行 flag 提交；

5、右上角显示竞赛倒计时，请各位选手注意时间节点。

6、需提前关注比赛规则，确认加固时长与混战时长，合理安排队伍内相关人员分工。