附件2

**大赛技术文件**

**目录**

**[一、 参赛对象 3](#_Toc566)**

**[二、 竞赛实施方案 3](#_Toc27252)**

**[2.1 竞赛组织规划 3](#_Toc17564)**

**[2.1.1 竞赛形式 3](#_Toc18155)**

**[2.1.2 竞赛规则 4](#_Toc29021)**

**[2.2 竞赛平台 6](#_Toc27952)**

**[三、 竞赛大纲 10](#_Toc15941)**

**[四、 竞赛说明 13](#_Toc5453)**

**一、参赛对象**

2025年“联通杯”陕西省数据安全管理员职业技能大赛暨第二届全国职工数字化应用技术技能大赛陕西省选拔赛面向全省从事数据安全工作的职工，考核选手在数据安全法规、数据安全技术应用、人工智能安全应用、数据安全攻防对抗以及前沿技术与新兴威胁等方面的综合能力，旨在提升人工智能时代下的数据安全保障水平。

**二、竞赛实施方案**

**（一） 竞赛组织规划**

1 .竞赛形式

大赛为个人赛，决赛共三场。第一场为理论赛、第二场为技能实操赛、第三场为综合场景赛，权重比为 3:3:4。

**第一场：数据安全理论赛（30%）**

本场比赛总分300分，比赛时长1小时，模式为数据安全理论赛，理论试题根据选手ID从系统题库中随机生成。理论考点主要包括数据安全的政策法规标准以及技术知识点。

**第二场：数据安全技能赛（30%）**

本场比赛总分300分，比赛时长2小时，模式为数据安全技能赛，数据安全技能赛分为数据安全题、数据分析题和模型安全题。知识点主要包括API接口安全、数据注入、数据高频采集、数据加解密、敏感数据识别、数据分类分级、数据脱敏、逆向分析、数据溯源与处置、模型数据安全等。

**第三场：数据安全综合场景赛（40%）**

本场比赛总分400分，共计3小时，模式为数据安全综合场景赛。通过虚拟仿真企事业单位真实网络环境、重要数据业务系统、人工智能模型的全流程业务场景及面临的典型数据安全攻击事件，考察选手对于企事业单位综合业务场景下的数据安全应用防护与研判分析能力、人工智能模型应用与数据安全分析能力。涉及的知识点有：数据采集安全、数据传输安全、数据存储安全、数据处理安全、数据交换安全、数据销毁安全、数据溯源与处置、逆向分析、人工智能模型数据安全与应用等。

2.竞赛规则

**第一场：**采用竞赛系统在线答题，数据安全理论赛题型包括单选题、多选题、判断题，参赛选手需根据题目描述，选择合适选项进行作答，选手需逐题点击提交，提交之后无法修改答案。

**第二场：**数据安全技能赛设置数据安全题、数据分析题和模型安全题三种题型，数据安全题预设指定“字符串”作为答案标识，选手通过各种技术手段分析获取答案，将答案提交至平台输入框即可，答对加分，答错不扣分；数据分析题采用大题小问形式，平台提供场景描述及题干要求，选手通过各种技术手段分析获取答案，将答案提交至平台对应题干下的输入框即可，答对加分，答错不扣分，限制答案提交次数为10次；模型安全题选手通过分析场景描述及要求完成解题，提交题干要求的附件至平台，选手主动点击题干下方的“提交答案”按钮选择对应需要提交的文件至平台，平台会自动进行答案验证，验证通过即可得分，验证不通过不扣分，平台限制验证次数为10次，系统实时统计分数并进行成绩展示。

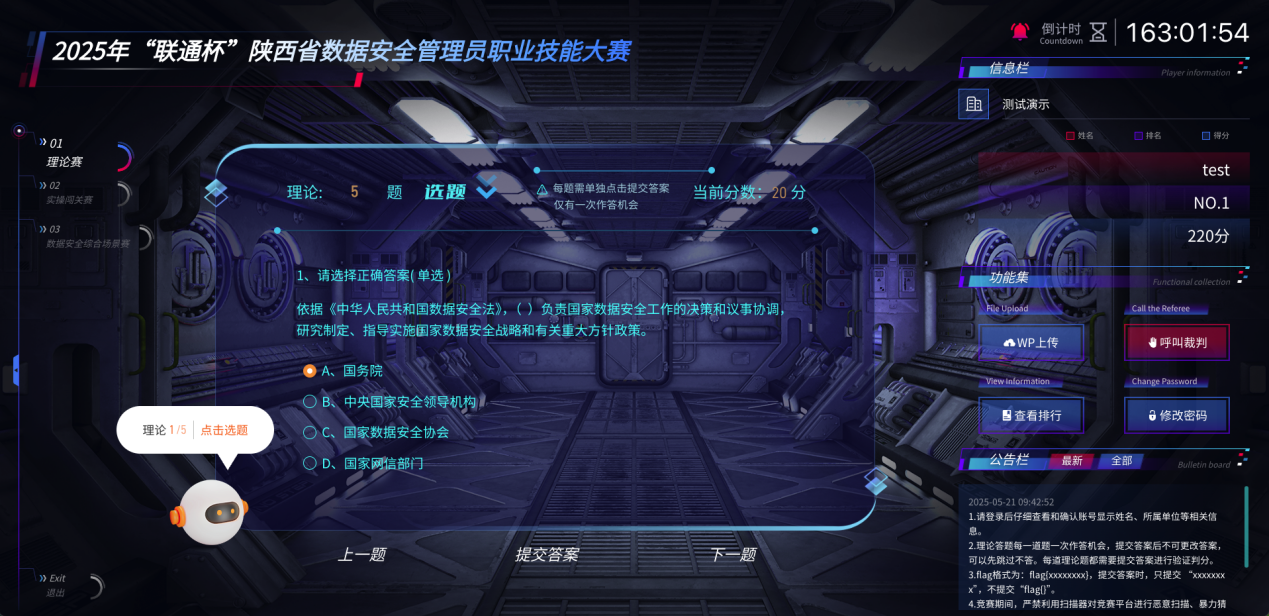
**第三场：**采用竞赛系统在线答题，竞赛平台将展示各参赛选手的IP地址段，考生需自己识别考题的网络拓扑结构，以便根据实际的场景进行题目作答，选手根据竞赛平台提供的题干描述以及提示进行答题，通过各种技术手段分析获取题干要求的答案，若答案格式要求为特定“字符串”标识，将“字符串”作为答案提交至平台输入框即可完成答题；若答案格式要求为特定“附件”，选手主动点击题干下方的“提交答案”按钮选择对应需要提交的文件至平台，平台会自动进行答案验证，验证通过即可得分，验证不通过不扣分，每道题限制为10次答题机会，系统实时统计分数并进行成绩展示。

选手个人总成绩=数据安全理论赛得分+数据安全技能赛得分+数据安全综合场景赛得分，竞赛排名按积分进行排序，积分相同的，则按时间进行排序，先得分的排名在前。

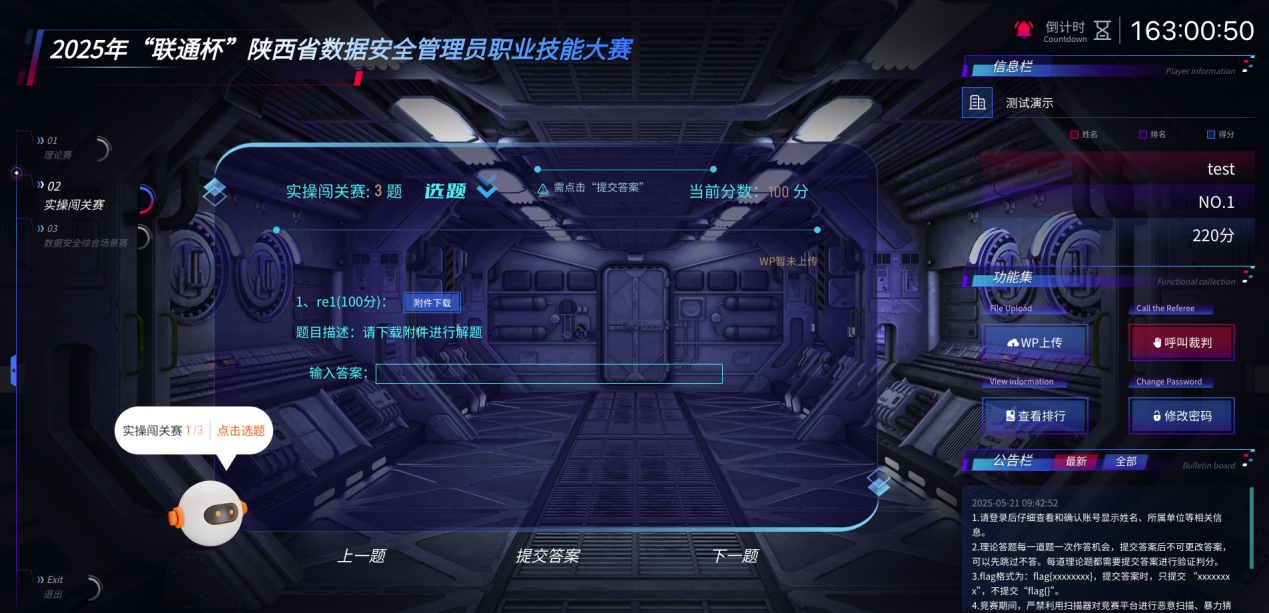
1. **竞赛平台**



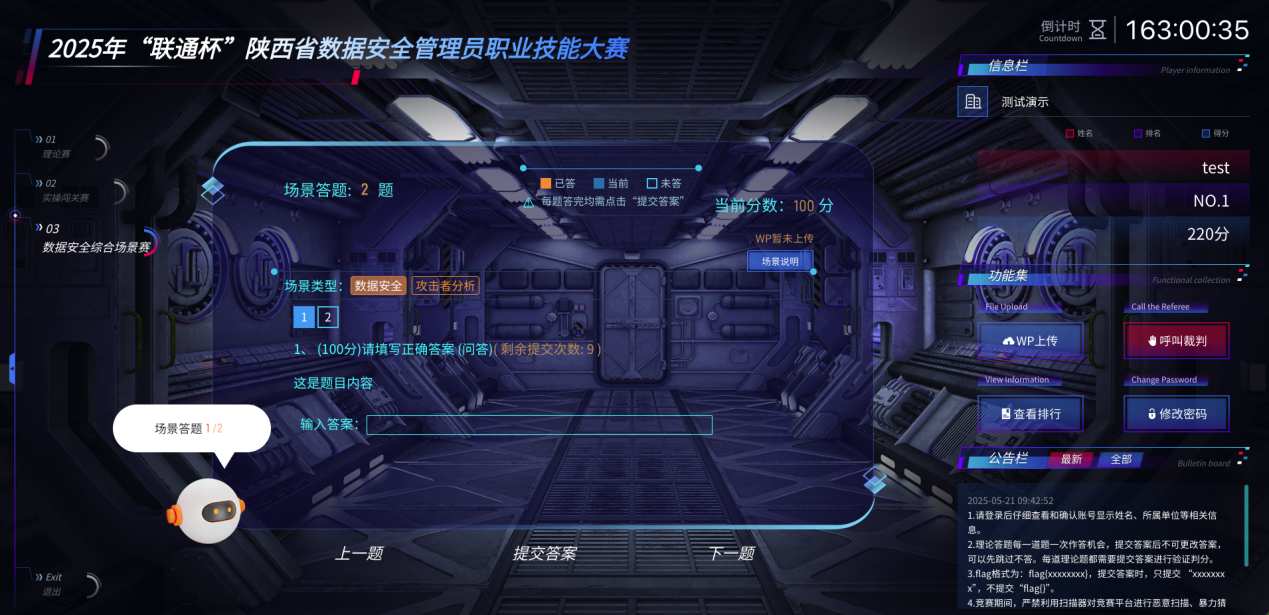
图：竞赛平台登录页面



图：数据安全理论赛答题页面



图：数据安全技能赛答题页面



图：数据安全综合场景赛答题页面





图：竞赛实时展示成绩页面主界面

**三、竞赛大纲**

1. **政策法规和标准体系**

掌握《中华人民共和国数据安全法》核心要求：数据分类分级制度、数据安全责任主体、数据安全风险评估与应急处置义务；

熟悉《中华人民共和国个人信息保护法》关键条款：最小必要原则、告知同意规则、个人信息跨境提供的安全评估要求、敏感个人信息处理限制；

了解《网络安全法》中与数据安全关联的内容；

掌握《关键信息基础设施安全保护条例》中涉及数据安全的要求；

熟悉《数据安全法》配套法规（如《数据出境安全评估办法》《个人信息出境标准合同办法》）的具体实施要求。​

掌握国家标准：GB/T 43697-2024《数据安全技术 数据分类分级规则》、GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型（DSMM）》等内容；

熟悉行业标准：金融行业《金融数据安全 数据安全分级指南》（JR/T 0197-2020）、医疗行业《卫生信息安全等级保护管理办法》等内容；

了解国际标准：ISO/IEC 27001（信息安全管理体系）、ISO/IEC 27701（隐私信息管理体系）、NIST SP 800-64（数据安全生命周期管理）、GDPR（欧盟通用数据保护条例）核心要求。

1. **数据安全全生命周期管理**

**1.数据采集阶段**​​

掌握合规采集原则、熟悉采集风险点、能识别违规采集行为，掌握采集安全技术等。

**2.数据传输阶段​​**

熟悉传输风险、掌握传输安全技术、了解传输安全工具。

**3.数据存储阶段​​**

掌握存储风险、熟悉存储安全技术、了解存储介质安全。

**4.数据使用阶段​​**

掌握使用风险、熟悉使用安全技术、了解使用场景安全。

**5.数据共享与销毁阶段​​**

掌握共享风险、熟悉共享安全技术、掌握销毁风险、熟悉销毁安全技术。

1. **数据安全核心的技术**

掌握分类分级方法、熟悉分类分级工具、能结合行业标准完成数据分类分级实战；

掌握静态脱敏、动态脱敏技术，熟悉匿名化技术，能评估脱敏效果；​

掌握加密技术：对称加密（AES、SM4）、非对称加密（RSA、SM2）、同态加密（全同态/部分同态），熟悉隐私计算技术：

掌握DLP核心技术、熟悉DLP工具部署、能分析DLP误报/漏报场景。

1. **人工智能安全技术基础​**

熟悉机器学习（监督/无监督/强化学习）、深度学习（CNN、RNN、Transformer）的核心原理与安全风险点；

掌握隐私计算技术（联邦学习、安全多方计算、同态加密）在AI中的应用场景（如跨机构联合建模、敏感数据协同分析）；

了解AI伦理与安全的关系（如算法偏见导致的歧视性决策、生成式AI的虚假信息传播风险）。

1. **人工智能安全技术核心​**

掌握对抗样本攻击（白盒/黑盒）与防御（对抗训练、随机平滑）、模型鲁棒性评估；

熟悉训练数据清洗（异常值检测、重复数据删除）、隐私保护（差分隐私在NLP/CV中的应用）、模型输出脱敏；

掌握大模型提示注入攻击（Prompt Injection）、越狱攻击（Jailbreak）的检测与防御（如指令微调、内容过滤）；

熟练使用AI安全工具（对抗样本生成工具Foolbox、模型评估工具IBM AIF360、隐私计算框架FATE）。

1. **其他**

熟悉密码技术的概念、加密体制的分类、常见加密方式、密码协议与密码分析工具的利用；

熟悉物联网、工业控制、无线、网络设备等相关方面的安全问题；

熟悉移动互联网恶意程序监测与处置机制，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；

掌握常见协议分析工具的使用，常见数据包分析方法；

熟练使用数据恢复的常用技术等相关知识点内容；

熟悉恶意代码的识别方法及防护措施。能运用相关技术发现、隔离、清除常见恶意代码；并能对常见恶意代码进行逆向分析。

**四、竞赛说明**

1. **竞赛须知**

1.请使用Firefox或者Chrome浏览器访问竞赛平台，其他

浏览器暂不兼容，可能会导致页面错位，无法提交Flag值。

2.使用浏览器访问竞赛平台时，请勿给浏览器设置代理，否

则Flag将无法提交验证。

3.理论答题每一道题一次作答机会，提交答案后不可更改答

案，可以先跳过不答，每道理论题都需要提交答案进行验证判分。

4.严禁利用扫描器对竞赛平台进行恶意扫描、或对竞赛平台

发起DDoS攻击。一经发现即刻封锁账号，取消参赛资格。

5.请勿利用手机、互联网相互通讯，禁止交流讨论，协同作

答。

6.如果对竞赛平台有疑问，或者对考题有疑义，或者其它与

竞赛相关的事宜，请举手示意，切勿大声呼喊。

1. **竞赛纪律（线下决赛）**

1.参赛队伍自行携带笔记本电脑、有线鼠标、RJ54网口转接头、键盘和本人身份证原件进入赛场，提前准备相关知识库与工具；

2.参赛队伍在竞赛开始前60分钟签到，竞赛正式开始后迟到者（迟到15分钟及以上）将不得进入竞赛场地；

3.竞赛座位按照事先分派决定，正式竞赛期间参赛选手不得

擅自离开竞赛座位，应举手请示工作人员，得到同意后方可离开自己竞赛座位；

4.竞赛开始前选手先测试网络是否正常，是否能够正常访问

比赛平台，如果无法正常访问比赛平台应及时举手等待现场工作人员帮助；

5.竞赛开始前选手手机一律上缴，由举办方暂时保管，比赛

结束后有秩序地领回自己手机。上缴前需提前安排好自身工作，若因手机上缴而影响个人工作导致重大后果的，举办方一律不承担相关责任；竞赛过程中，如果发现选手将手机带入考场座位，按作弊处理。

6.竞赛过程中禁止选手接入互联网，禁止通过互联网查找资

料，禁止通过任何形式寻求网络外援远程协助答题，发现违规者一律取消参赛资格；

7.比赛过程中禁止使用通用防御脚本/工具防御对手攻击，

一旦被检测并查实使用通用防御则进行扣分并警告，经警告3次仍然不撤销通用防御队伍决赛记0分；

8.竞赛过程中或竞赛后如有任何问题（包括反映竞赛或其它

问题），应立即举手示意，等待现场工作人员帮助；

9.比赛过程中，不同队伍之间不允许以任何形式相互讨论、

交流、合作、分享资料，一经发现直接取消比赛资格，相关队伍立刻离场；

10.任何时候禁止攻击裁判服务器，否则将判令停止比赛，

决赛分数为0分；

11.比赛过程中应遵守赛场秩序，禁止大声喧哗影响其他队伍比赛；

12.比赛过程中以及比赛结束后裁判有权抽查参赛选手解题方法/得分思路，如果发现回答有误，疑似通过作弊获得分数将对参赛选手扣分，严重者取消参赛资格；

13.裁判组将视情况对违反比赛纪律的行为采取禁赛、取消比赛成绩等处罚措施，情节严重者将在行业内通报。