第十八届全国大学生信息安全竞赛

创新实践能力赛Build环节

（知识库构建与安全检测项创新设计）

赛前须知

随着网络硬件设备和大模型在企业应用中的广泛部署，由漏洞与配置缺陷导致的安全问题日益突出。为此，本届比赛Build环节设置知识库构建和安全检测项创新设计任务，旨在检验选手收集整合信息的能力和安全检测项创新设计能力。

大赛将针对Build环节设置创新单项奖，同时Build环节的成果也将在赛后分享给所有参赛队伍。

一、基本信息

时间	环节	内容
7月4日10:00 -7月5日18:00	Build环节 第一次提交 （线上）	1.完成知识库构建与安全检测项创新设计 2.7月8日公布第一次Build环节成绩
7月11日10:00 -7月12日18:00	Build环节 第二次提交 （线上）	1.完成知识库构建与安全检测项创新设计 2.7月16日公布第二次Build环节成绩

比赛形式：线上比赛

平台地址：https://match.ichunqiu.com/2025build （7月4日10:00开放访问）

登录方式：报名预留手机号+验证码

二、赛制介绍

比赛内容包括两个任务：

（1）知识库构建任务：围绕设定的网络硬件设备方向、大模型安全方向，梳理相关安全信息，进行数据清洗与归类整合，最终提交具备组织性、实用性的知识库；

（2）安全检测项设计任务：依据主办方给定的基础检测项，针对企业内网环境安全设计新增检测项，以补充完善企业内网整体安全检测体系，最终提交包含原有及新增检测项的检查项测试集。

2.1 知识库构建任务

2.1.1 任务背景

随着网络硬件设备和大模型在企业应用中的广泛部署，其安全问题日益突出。网络硬件设备和大模型安全频现漏洞与配置缺陷。为此，本任务聚焦网络硬件设备方向和大模型安全方向，梳理漏洞与攻击案例，进行数据清洗与分类整合，构建具备组织性、实用性的安全知识库，为提升系统安全防护能力提供基础支撑。

2.1.2 任务目标

本任务旨在引导选手围绕网络硬件设备与大模型安全两个方向构建结构化知识库：

一方面，聚焦2020年起Cisco、TP-LINK等主流硬件设备以及车联网设备的漏洞信息，提取CVE编号、攻击向量、补丁链接等要素并分类整理；

另一方面，围绕ChatGPT、文心一言等大模型，系统梳理2023年起公开的提示注入、越狱等攻击技术与防御方案。

2.1.3 任务要求

（1）构建知识库分为2个方向：

- 网络硬件设备漏洞
- 大模型安全漏洞

（2）网络硬件设备漏洞内容必须包含以下要素：

- 序号
- 设备品牌
- 设备类型
- 产品型号
- CVE编号
- 漏洞描述
- 攻击向量
- 厂商补丁链接

•受影响版本

•公开日期

注意：设备类型为路由器、交换机、防火墙、IDS、IPS之类的设备品牌，收集范围**包含但不限于**Cisco、TP-LINK、NETGEAR、ASUS、D-Link；设备类型为车载通信网关、车载信息娱乐系统、V2X通信模块、OTA升级模块、FOTA管理模块、CAN总线控制器等车联网相关设备的品牌不做限制。

（3）大模型安全漏洞内容必须包含以下要素：

•序号

•模型名称

•厂商

•攻击类型

•攻击名称

•攻击方式描述

•是否有PoC

•修复方案

•防御技术

•公开日期

注意：模型名称**包括**ChatGPT、Gemini、Claude、Llama、

文心一言、通义千问等；攻击类型包括提示注入、越狱、命令注入等。

（4）网络硬件设备漏洞至少包含 50 个漏洞信息，大模型安全漏洞至少包含 30 个漏洞信息，收集漏洞信息的数量可扩展，数量不限。

2.1.4 测试项样例表

提交的 Excel 文档包含 2 个 sheet。

Sheet1：网络硬件设备安全知识库

序号	设备品牌	设备类型	产品型号	CVE 编号	漏洞描述	攻击向量	厂商补丁链接	受影响版本	公开日期
1	Cisco	交换机	Cisco 550X Series Stackable Managed Switches	CVE-2020-3121	Web-based 管理界面存在 XSS 漏洞，允许攻击者执行任意脚本	网络远程	Cisco Advisory: cisco-sa-20200122-sbsms-xss	所有未应用补丁的 Smart/Managed Switch 系列	2020 年 1 月 22 日
2	Cisco	路由器	Cisco IOS XE（ASR 903 + RSP3C）	CVE-2025-20189	ARP 处理内存管理缺陷，允许未经认证的邻接攻击者触发 DoS，导致 RSP 重载/重启	邻接网络发送构造 ARP 消息	Cisco Advisory: cisco-sa-asr903-rsp3-arp-dos-WmfzdvJZ	ASR 903 上运行的 IOS XE（尚未更新补丁前）	2025 年 5 月 7 日
3	Digitalcom	车载通信网关	Syrus4 IoT 网关	CVE-2023-6248	未授权 MQTT 可执行任意命令，泄露敏感数据	网络（MQTT 无认证）	联系厂商获取更新	所有连接云端设备	2023 年 11 月 21 日
4	GM	信息娱乐系统	MyLink（Equinox 2021）	CVE-2023-28885	播放恶意 MP3 导致系统 DoS	USB/媒体播放	无官方补丁，建议更新系统	build 2021.3.26	2023 年 3 月 27 日

Sheet2：大模型安全知识库

序号	模型名称	厂商	攻击类型	攻击名称	攻击方式描述	是否有PoC	修复方案	防御技术	公开日期
1	ChatGPT	OpenAI	提示注入	策略木偶攻击	通过伪造策略文件格式（如 XML/INI）绕过安全规则，诱导模型生成有害内容	是	升级 API 参数校验逻辑，强化输入清洗规则	输入过滤+字符转义+意图识别	2023 年 6 月 1 日
2	Gemini	Google	越狱	多步骤逻辑诱导	通过虚构故事逐步突破选举相关防御，利用模型逆缩放特性泄露系统提示	是	新增安全层拦截递归对话，限制多轮交互深度	动态检测+对话历史分析	2023 年 12 月 1 日

2.1.5 提交方式

开赛后，在规定时间内依据 Build 任务内容描述，完成收集网络硬件设备漏洞与大模型安全漏洞知识库，按照模板在平台对应的题目处提交 1 个 Excel 文档。

文件名格式：队伍编号_知识库构建_提交轮次.xlsx（如：T0001_知识库构建_第一轮.xlsx）。

提交前将 xlsx 文件打包成 zip 包（文件名随意）再提交到平台。

2.1.6 评分标准

选手围绕网络硬件设备与大模型安全两个方向构建结构化知识库并提交，每一轮赛后平台方将知识库应用到大模型并且进行训练，并由专家评审团从平台方知识库中选取 10 道固定题与

5 道随机题对训练后的模型进行提问，依据回答中技术要点的准确性及内容完整性进行评分，每题 1 分，满分 15 分。（原有样例不计入评分）。

	网络硬件设备安全	大模型安全	合计
固定题	7 道	3 道	10 道
随机题	3 道	2 道	5 道

2.2 安全检测项设计任务

2.2.1 任务背景

随着网络安全威胁持续演化，内网作为企业网络的核心区域，其安全防护尤为关键。传统的内网检测手段往往存在盲区，难以全面覆盖实际攻击面。本任务旨在引导选手围绕真实攻防需求，设计具有实战意义的内网安全检测项，增强检测体系的全面性和针对性。

2.2.2 任务目标

选手需在已提供的基础检测项基础上，设计新增内网安全检测项，通过对实际攻击行为、系统配置、用户行为、网络通信等多维度的分析，提出合理、必要、具备执行性的检测内容。

2.2.3 任务要求

（1）检测内容分为5个方向：

•信息收集

•漏洞扫描

•应用安全

•主机安全

•应急响应

（2）每项检测内容必须包含以下要素：

•测试项

•测试步骤

（3）每个基础检测项中最多计分10个有效测试项（不包含原有样例测试项），并且这些测试项属于该检测项的范围，新增检测项设计数量不限，但每支队伍最多计分50个有效的测试项。

（4）所提交内容需结构清晰、逻辑完整，具备实战可行性。

（5）所有新增检测项将在每一轮赛后由专家评审团进行审核。

2.2.4 测试项样例表

序号	检测内容	测试项	测试步骤
1	信息收集	Web应用的指纹识别	使用WhatWeb、Wappalyzer等工具分析目标网站的Web服务器类型（如Apache、Nginx）、CMS（如WordPress、Drupal）、框架（如Django、Laravel）及前端技术（如React、Vue.js）。

			检查 HTTP 响应头，提取 Server、X-Powered-By 等字段，确认技术版本信息。 使用 dirsearch 工具扫描 robots.txt、sitemap.xml 等文件，寻找隐藏路径或敏感文件。
2	漏洞扫描	SQL 漏洞检测	1. 使用 sqlmap 扫描目标网站的 URL 参数、POST 数据或 Cookie，检测是否存在 SQL 注入漏洞（命令示例：sqlmap -u "http://target.com/page?id=1" --batch）。 2. 验证潜在注入点，尝试不同类型的 SQL 注入（如基于错误、布尔、时间延迟），确认可利用性（示例：sqlmap -u "http://target.com/page?id=1" --technique=BEUST）。 3. 若发现漏洞，提取数据库信息（如版本、表名、数据），记录漏洞详情并测试是否可获取敏感数据。
3	应用安全	水平越权检测	1. 使用低权限用户账户（如普通用户）登录系统，获取用户 ID 或其他标识参数（如 URL 中的 user_id 或 Cookie 中的会话 ID）。 2. 尝试修改请求中的用户 ID（通过 Burp Suite 拦截修改 GET/POST 参数），访问其他用户的数据（如个人信息、订单记录）。 3. 验证是否能访问或修改不属于当前用户的数据，记录越权漏洞详情（如可访问的敏感信息或可执行的操作）。
4	主机安全	密码安全测试	1. 使用 Nmap 或 Metasploit 扫描目标服务器开放的服务（如 SSH、RDP、FTP），识别支持密码认证的服务（命令示例：nmap -p 22,3389 target_ip）。 2. 使用 Hydra 或 Medusa 对服务进行密码爆破测试，尝试常见密码字典（如 rockyou.txt）或弱口令（示例：hydra -L users.txt -P passwords.txt ssh://target_ip）。 3. 检查密码策略，验证是否启用复杂性要求、定期更换和账户锁定机制。
5	应急响应	windows 用户排查	1. 使用 PowerShell 或 CMD 列出所有用户账户，检查是否存在异常或未经授权的账户（命令示例：net user 或 Get-LocalUser）。 2. 检查管理员组成员，验证是否有可疑账户被添加到高权限组（命令示例：net localgroup Administrators）。 3. 分析用户登录日志，查看最近登录时间和来源，识别异常登录行为 。 4. 检查隐藏用户：查看注册表 HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names 。

2.2.5 提交方式

开赛后，在规定时间内依据 Build 任务内容描述，完成安全检测项设计，按照模板在平台对应的题目处提交 1 个 Excel 文档。

文件名格式：队伍编号_安全检测项设计_提交轮次.xlsx（如：

T0001_安全检测项设计_第一轮.xlsx）。

提交前将 xlsx 文件打包成 zip 包（文件名随意）再提交到平台。

2.2.6 评分标准

选手根据基础检查项补充并完善新的检测项，每一轮赛后由专家评审团确认新设计的检测项为必要增加内容，给出相应分值。每新增 1 个有效检测项得 1 分，最高得分为 50 分。

2.3 总成绩计分规则

Build 环节总成绩=（知识库构建分数/最高知识库构建分数）*80 分+（安全检测项设计分数/最高安全检测项设计分数）*20 分

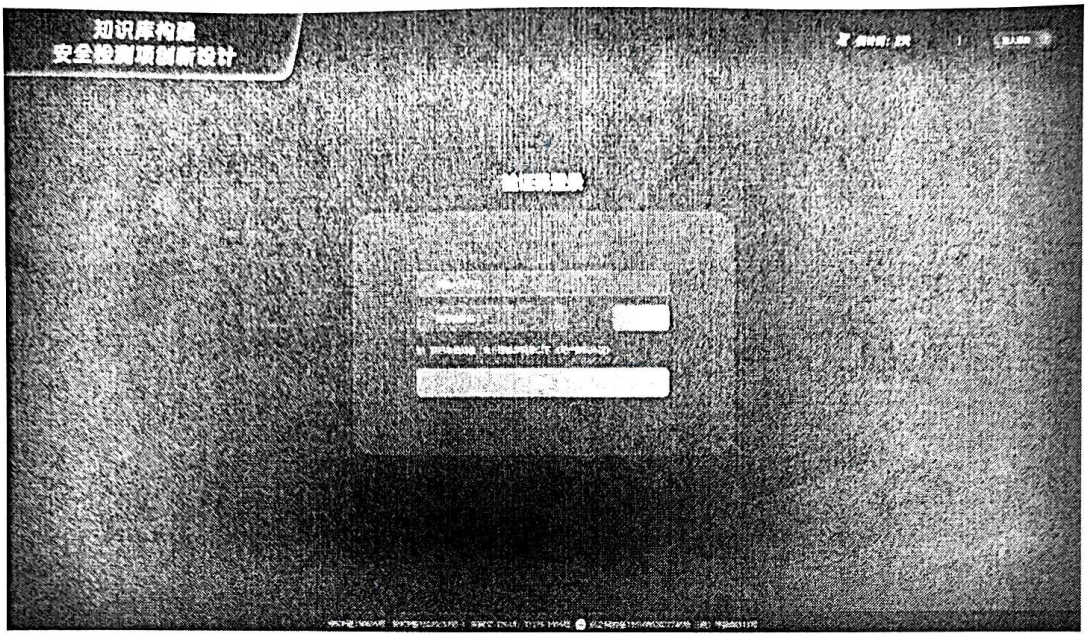
Build 环节有两个提交的时间段，第二轮可优化第一轮的提交内容后重新提交，最终成绩取两轮中最高分。

注*Build 环节不设立并列名次，名次按照所得分数从高到低排列，同分数情况下相对的用时较短者排名在前。

三、操作指南

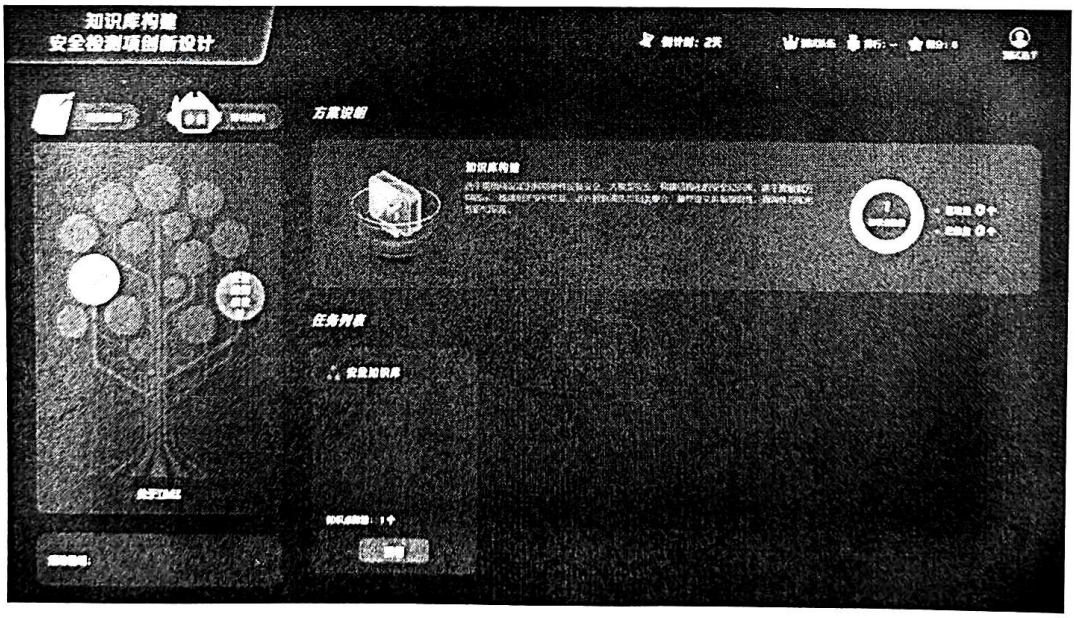
3.1 平台登录

比赛登录界面如下图所示：



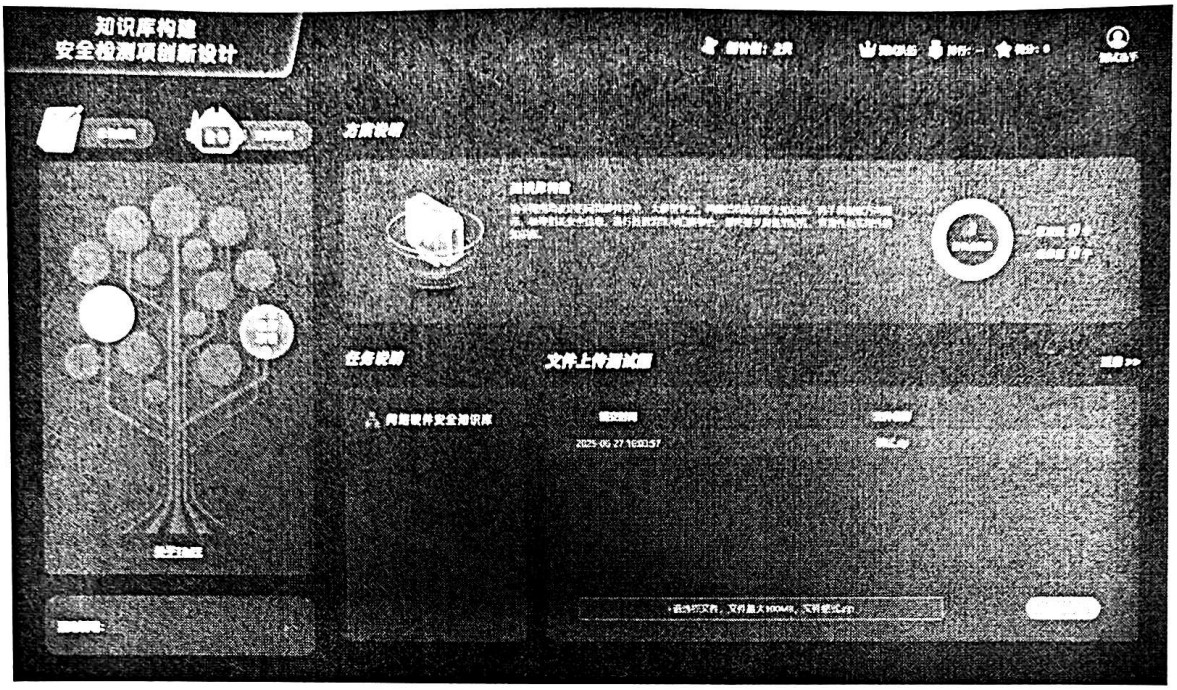
3.2 答题界面

点击题目图标即可进入，选手可自由选择答题顺序。



3.3 上传文件

点击“上传文件”，提交对应文件。注意：文件大小不超过100MB，文件格式为“.zip”。



注*以上图片均为示例

选手提交完后，等待平台公布成绩。每个任务可以提交多次，但每一轮只对选手最后一次提交做评审。

四、注意事项

参赛团队须独立完成全部构建与设计内容，严禁复制抄袭其他队伍成果。

如遇赛程中遇到任何问题，选手可通过竞赛官方QQ群（1046816089），联系群内工作人员。

本Build环节的相关规则及未尽事宜，最终解释权归第十八届全国大学生信息安全竞赛——创新实践能力赛组委会所有。

检测项样例表附件：

检测项样例表.zip

第十八届全国大学生信息安全竞赛

创新实践能力赛竞赛组委会

（郑州大学网络空间安全学院 代章）

2025 年 7 月