



中国认可
国际互认
检测
TESTING
CNAS L21630

检测报告

Testing Report

(未经允许, 不得部分复制本报告)

产品名称: 壹信 IM 后端系统

产品类型: 应用软件

检测类别: 委托测试 (产品质量-信息安全性
(代码审计))

委托单位: 济南壹软网络科技有限公司

发布日期: 2026 年 8 月 14 日

深圳市一航网络信息技术有限公司

公司地址: 广东省深圳市南山区科技路1号桑达科技大厦2层206B

声 明

1、本报告是深圳市一航网络信息技术有限公司对委托项目进行软件全面质量测试后得出的客观结论。

2、本报告的结论仅对测试时间段内委托系统现有的状况有效。

3、本报告中给出的结论，不得作为对委托系统内关联产品的结论。

4、本报告未经被测单位和深圳市一航网络信息技术有限公司书面允许不得节选和复印，复印件需重新加盖“深圳市一航网络信息技术有限公司检验检测专用章”才有效。

5、任何情况下，若需引用本报告中的内容都应保持其本来意义，不得擅自增加、修改、伪造或掩盖本报告的原有内容。

6、本报告无“深圳市一航网络信息技术有限公司检验检测专用章”无效，涂改无效；报告无主检人、审核人和批准人签字无效。

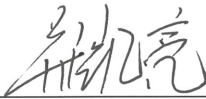
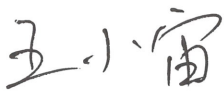
7、本报告已经过区块链技术全流程上链存证和保护，区块链证书验真请扫描报告上的二维码或直接官网输入报告查询码进行查询验证。

8、对本报告如有异议，可于收到报告之日起十五日内向我单位提出申诉。

9、本报告一式贰份，壹份提交委托单位，壹份留存深圳市一航网络信息技术有限公司。

检测报告总表

产品名称	壹信 IM 后端系统	版本号	V1.0
样品编号	2be68dac-01	产品编号	——
样品状态	完好	样品数量	1
委托单位	济南壹软网络科技有限公司	委托单位 联系地址	山东省济南市天桥区药山 街道二环西路与二环北路 交叉口海信云创中心 2 号 楼 1 单元 420 室
开发单位	济南壹软网络科技有限公司	开发单位 联系地址	山东省济南市天桥区药山 街道二环西路与二环北路 交叉口海信云创中心 2 号 楼 1 单元 420 室
接收日期	2026 年 8 月 11 日		
检测日期	2026 年 8 月 11 日-2026 年 8 月 12 日		
检测地点	广东省深圳市南山区科技路 1 号桑达科技大厦 2 层 206B 深圳市一航网络信息技术有限公司		
检测类别	委托测试（产品质量-信息安全性（代码审计））		
检测依据	国家标准： GB/T 25000.51-2016 《系统与软件工程 系统与软件质量要求和评价（SQuaRE）第 51 部分：就绪可用软件产品（RUSP）的质量要求和测试细则》		
结论	本次针对“济南壹软网络科技有限公司”委托的“壹信 IM 后端系统”按照国家标准：GB/T 25000.51-2016 《系统与软件工程 系统与软件质量要求和评价（SQuaRE）第 51 部分：就绪可用软件产品（RUSP）的质量要求和测试细则》，结合《委托测试申请表-壹信 IM 后端系统》、《用户手册-壹信 IM 后端系统》从信息安全性方面对软件进行检测，以验证系统符合安全需求定义和质量标准。 经检测，壹信 IM 后端系统符合软件产品的需求定义和质量标准，测试通过。		

	测试结果： ☒ 通过 ☐ 不通过 深圳市一航网络信息技术有限公司 		
发布日期	2026 年 8 月 14 日		
拟 制		审 核	
测试人员		批 准	
备 注	——		

目 录

第 1 章 测试概述	7
1.1 委托单位信息	7
1.2 检测机构信息	7
1.3 测试范围	8
1.3.1 信息安全性测试	8
1.4 引用文档	8
1.5 测试计划	8
1.6 测试方法	8
1.7 测试工具	9
1.8 人员配置	9
第 2 章 系统概况	11
2.1 测试系统	11
2.2 软/硬件环境及配置	11
2.3 软件规模及开发语言	11
第 3 章 测试通过准则	12
3.1 缺陷等级划分表	12
3.2 测试结论与缺陷处理	12
第 4 章 测试执行情况	13
4.1 测试用例通过情况概述	13
4.1.1 信息安全性测试	13
4.2 不确定度	13
4.3 测试用例执行情况分析	13
4.3.1 首轮测试	13
4.4 测试缺陷统计	14
4.4.1 首轮测试	14
第 5 章 测试总结	15
5.1 问题/风险及建议	15
5.2 测试结论	15
第 6 章 附录-测试记录	16
6.1 产品质量-信息安全性测试结果及截图	16
6.1.1 代码审计	16

第 1 章 测试概述

“壹信 IM 后端系统”是面向即时通信业务的服务端软件，提供账户认证、设备与联系人管理、私聊、群聊、频道、消息发送与同步、WebSocket 实时推送、动态、钱包会员、音视频通话及会议控制、运营管理、客服和机器人等接口。系统采用 Go/Gin 开发，MySQL 存储业务关系与运营数据，MongoDB 存储消息文档，Redis 用于缓存、限流、队列和在线状态，支持通过 Docker Compose 在 Linux amd64/arm64 环境隔离部署。本次送测仅包含后端源码、数据库结构和脱敏测试环境，不含客户端及 Vue 管理前端。

受济南壹软网络科技有限公司的委托，深圳市一航网络信息技术有限公司（以下简称“一航网络”）组建了《壹信 IM 后端系统》软件测试工作组（以下简称“工作组”），于 2026 年 8 月 11 日至 2026 年 8 月 12 日对《壹信 IM 后端系统》进行全范围的软件产品信息安全性测试。

本次测试针对壹信 IM 后端系统提供的安全模块进行了详细测试，基本做到了该产品在安全测试类型和场景的全覆盖。

本报告是在完成《壹信 IM 后端系统》软件产品质量测试后，对测试记录深入分析的基础上，客观的描述与判断测试系统在信息安全性方面存在的缺陷。

1.1 委托单位信息

单位名称：济南壹软网络科技有限公司；

联系地址：山东省济南市天桥区药山街道二环西路与二环北路交叉口海信云创中心 2 号楼 1 单元 420 室；

联系人员：董腾霄；

联系电话：18888328857。

1.2 检测机构信息

单位名称：深圳市一航网络信息技术有限公司；

联系地址：广东省深圳市南山区科技路 1 号桑达科技大厦 2 层 206B；

服务热线：400-870-6298；

联系人员：郭雯雯；

联系电话：17620343198。

1.3 测试范围

1.3.1 信息安全性测试

序号	测试项	测试项说明
1	代码审计	代码审计未发现安全漏洞风险问题。

1.4 引用文档

- ✓ GB/T 25000.51-2016 《系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第 51 部分：就绪可用软件产品（RUSP）的质量要求和测试细则》
- ✓ 委托测试申请表-壹信 IM 后端系统
- ✓ 用户手册-壹信 IM 后端系统

1.5 测试计划

本次测试为软件产品信息安全性测试，测试计划时间为：2026 年 8 月 11 日-2026 年 8 月 12 日。

1.6 测试方法

1、信息安全性测试（A）：通过白盒（代码审计）的方式检查应用系统的安全性。

2、白盒测试（B）：工具审查+人工确认+人工抽取代码检查，依照“OWASP、PCI、CWE、SANS25、SOX、GDPR 等国际代码安全组织策略标准”所披露的脆弱性，根据业务流来检查目标系统的脆弱性、缺陷以及结构上的问题。

1.7 测试工具

测试硬件设备			
设备名称	Acer 宏碁电脑		
设备配置	I7/8GDDR/500G SSD 硬盘		
测试软件工具			
设备名称	版本号	生产商/来源	用途
Fortify Audit Workbench	23.2.0.0083	Micro Focus	代码审计工具

1.8 人员配置

序号	角色	姓名	备注
1	项目负责人	欧志	1、评审并批准项目计划及有关报告； 2、组织并确保团队工作； 3、控制项目执行； 4、评估项目绩效； 5、与有关人员进行沟通。
2	测试组长	王小宙	1、项目计划编制； 2、协调并实施项目计划中； 3、确定的活动； 4、识别测试环境需求； 5、负责设计测试用例； 6、为其他人员提供技术支持。
3	测试人员	郑凯亮	1、执行测试活动； 2、在项目计划制订阶段，识别项目活动； 3、估计每项活动所需的时间。
4	质量监督员	王小宙	1、确定项目质量目标； 2、制订并实施质量计划； 3、监督、指导项目活动的执行过程。

5	配置管理员	陈俊华	1、提供资源保障； 2、建立并维护测试环境。
---	-------	-----	---------------------------

第 2 章 系统概况

2.1 测试系统

测试样品名称：壹信 IM 后端系统样品
系统全称：壹信 IM 后端系统

2.2 软/硬件环境及配置

序号	硬件环境		软件环境
	名称/型号	配置（芯片/内存/硬盘）	
1	隔离检测服务器	CPU： Intel i5 内存： 8GB 硬盘： 512GB SSD	操作系统：Linux 数据库：mysql8.0 / MongoDB7.0 中间件：Redis7-alpine

2.3 软件规模及开发语言

软件名称/版本	壹信 IM 后端系统
开发语言	Go
开发平台	Docker Engine 24+； Docker Compose v2
运行平台	Linux

第3章 测试通过准则

3.1 缺陷等级划分表

严重性等级/名称		说 明
1 级	致命	不能执行正常功能或重要功能，或者危及人身安全。
2 级	非常严重	严重地影响系统要求或基本功能的实现，且没有办法解决。
3 级	严重	严重地影响系统要求或基本功能的实现，但存在合理的解决办法。
4 级	一般	使操作者不方便或遇到麻烦，但不影响执行工作功能或重要功能。
5 级	轻微	其他错误。

3.2 测试结论与缺陷处理

- 1) 测试结论分为通过和不通过。
- 2) 当检测的安全测试项发现中级或中级以上安全风险问题，测试为不通过。
- 3) 当所有检测的测试项均为通过时，测试结论为通过，否则为不通过。

第 4 章 测试执行情况

4.1 测试用例通过情况概述

4.1.1 信息安全性测试

4.1.1.1 代码审计

序号	测试项	测试项说明	测试结果	备注
1	代码审计	代码审计未发现紧急风险、高危风险和中危风险以上安全风险问题。	通过	详细请参见第 6 章附录-测试记录。

4.2 不确定度

本报告中的符合性判定仅依据实验室环境下的检测结果，不考虑其检测结果的不确定度。

4.3 测试用例执行情况分析

4.3.1 首轮测试

产品名称	壹信 IM 后端系统			
测试类型	信息安全性测试（代码审计）			
测试情况	计划测试项数	实际执行测试项数	已通过测试项数	未通过测试项数
	97	97	97	0
合计	97	97	97	0

4.4 测试缺陷统计

4.4.1 首轮测试

缺陷归属	测试类型	缺陷数量	缺陷程度数量			
			致命	严重	一般	轻微
壹信 IM 后端系统	信息安全性测试 (代码审计)	0	0	0	0	0

第 5 章 测试总结

5.1 问题/风险及建议

序号	问题/风险归属	问题/风险描述	严重性	应对措施	责任人
1	壹信 IM 后端系统	——	——	——	——

5.2 测试结论

- 1、系统各项测试正常，测试过程未发现问题；
 - 2、系统满足 GB/T 25000.51-2016 《系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第 51 部分：就绪可用软件产品（RUSP）的质量要求和测试细则》；
- 综上：壹信 IM 后端系统符合软件产品的需求定义和质量标准，测试通过。

第 6 章 附录-测试记录

6.1 产品质量-信息安全测试结果及截图

6.1.1 代码审计

6.1.1.1 源代码基本信息

序号	压缩包名称	验证码 (MD5)	规格(行)	备注
1	yixinim-backend-security-test-delivery-20260810.zip	788d082e6c73e1471d4c33bceb82da51	53,095	初次测试

6.1.1.2 审计原则

开展的代码安全审计工作中，审计过程遵循以下原则：

1) 标准性原则：审计方案的设计和实施都在充分吸纳国家标准如：审计依据标准 GB/T 25000.51-2016：《系统与软件工程 系统与软件质量要求和评价（SQuaRE）第 51 部分：就绪可用软件产品（RUSP）的质量要求和审计细则》、GB/T 39412-2020：《信息安全技术 代码安全审计规范》的“信息安全性”基础上进行。

2) 规范性原则：审计工作中的过程和文档，严格按照国家规范操作，严格执行项目的跟踪和质量控制。

3) 可控性原则：审计过程和所使用的工具具有可控性。

4) 整体性原则：审计服务从组织的实际需求出发，结合业务需求、安全管理和业务运营等方面进行代码安全审计，而不是仅仅局限于网络、主机等单个的安全层面。

5) 最小影响原则：审计实施过程中制定充分细致的工作计划，尽可能不对现网的运行和业务的正常运转产生显著影响，同时采取必要控制措施尽可能小地

影响系统和网络的正常运行。

6) 保密性原则：从公司、人员、过程三个方面进行保密控制：公司双方签署保密协议，不得利用产品质量-信息安全性（代码审计）中的任何数据进行其他有损甲方利益的用途；所有参与项目的人员签订个人保密协议；在产品质量-信息安全性(代码审计)检测过程中对审计相关的数据执行严格的保密控制措施；项目结束后确保有关敏感数据被安全清除。

6.1.1.3 审计流程

审计流程主要包括以下阶段：

签署产品质量-信息安全性（代码审计）授权书

确定范围：根据审计需要，确定本次项目的范围；允许使用的攻击手段。是否允许使用暴力破解、拒绝服务等手段；

安全漏洞检查阶段：这是整个评估过程中花费时间最长的一个阶段，安全工程师利用代码审计、端口扫描、漏洞扫描等工具对产品质量-信息安全性（代码审计）检测的目标进行安全漏洞检查，并根据扫描结果筛选可以利用的漏洞；

代码审计阶段。安全工程师针对发现的漏洞，利用攻击程序进行攻击审计。例如：验证漏洞存在并取证，则结束产品质量-信息安全性（代码审计）检测过程。如果所有的攻击审计都没有成功，可以根据需要选择使用其他手段进行更进一步的审计，或者直接结束审计过程。

6.1.1.4 漏洞识别

针对安全评估发现的安全漏洞，确定风险等级。风险等级依照后果的不同严重程度分为5级，分别是很高、高、中等、低和很低级。下表为风险等级划分的说明：

等级	标识	描述
5	很高	风险发生的可能性很高，对系统资产产生很高的影响
4	高	风险发生的可能性很高，对系统资产产生中等及高影响
		风险发生的可能性高，对系统资产产生高及以上影响
		风险发生的可能性中，对系统资产产生很高影响
3	中等	风险发生的可能性很高，对系统资产产生低及以下影响
		风险发生的可能性高，对系统资产产生中及以下影响

		风险发生的可能性中，对系统资产产生高、中、低影响
2	低	风险发生的可能性中，对系统资产产生很低影响 风险发生的可能性低，对系统资产产生低及以下影响 风险发生的可能性很低，对系统资产产生中、低影响
1	很低	风险发生的可能性很低，发生后对系统资产几乎无影响

GB/T 20984-2022 《信息安全技术 信息安全风险评估方法》 风险等级划分表

6.1.1.5 审计项目

本次主要审计项目包括但不限于以下安全缺陷审计检查列表：

一、安全功能缺陷审计（37 条审计条款）

序号	审计项/审计条款			审计指标
1	数据清洗	输入验证	关键状态数据外部可控	应避免关键状态数据被外部控制
2			数据真实性验证	宜验证数据真实性，避免接收无效数据
3			绕过数据净化和验证	宜防止以大小写混合的方式绕过数据净化和验证
4			在字符串验证前未进行过滤	不宜在过滤字符串之前对字符串进行验证
5			对 HTTP 头 Web 脚本特殊元素处理	应对 HTTP 头的 Web 脚本语法中的特殊元素进行过滤和验证
6			命令行注入	应正确处理命令中的特殊元素
7			数据结构控制域安全	应避免对数据结构控制域的删除或意外增加。
8			忽略字符串结尾符	应保证字符串的存储具有足够的空间容纳字符数据和结尾符
9			对环境变量长度做出假设	不应对环境变量的长度做出假设
10			条件比较不充分	执行比较时不应部分比较或不充分的比较
11			结构体长度	不应将结构体的长度等同于其各个成员长度之和
12			数值赋值越界	应避免数值赋值越界
13			除零错误	应避免除零错误
14			边界值检查缺失	数值范围比较时，不宜遗漏边界值检查
15			数据信任边界的违背	代码应避免将可信和不可信数据组合在同一结构体中，违背信任边界

16			条件语句缺失默认情况	条件语句中不宜缺失默认情况
17			无法执行的死代码	不宜包含无法执行的死代码
18			表达式永真或永假	不应出现表达式永真或永假代码
19		输出编码	跨站脚本	应避免跨站脚本攻击
20			Web 应用重定向后执行额外代码	Web 应用不宜在重定向后执行额外代码
21			URL 重定向	不应开放不可信站点的 URL 重定向
22	数据加密与保护	数据加密	密码安全	密码相关实现技术应符合国家密码相关管理规定
23			随机数安全	应确保产生安全的随机数
24			使用安全相关的硬编码	不应使用安全相关的硬编码
25		数据保护	敏感信息暴露	应避免敏感信息暴露
26			个人信息保护	应确保个人信息保护
27	访问控制	身份鉴别	身份鉴别过程中暴露多余信息	应避免在处理身份鉴别的过程中暴露多余信息
28			身份鉴别被绕过	应避免身份鉴别被绕过
29			身份鉴别尝试频率限制	应对身份鉴别连续多次登录失败频率进行限制
30			多因素认证	宜使用多因素认证机制
31		口令安全	登录口令	应确保登录过程中口令不可明文显示
32			明文存储口令	应避免明文存储口令
33			明文传递口令	应避免明文传递口令
34		权限管理	权限访问控制	应确保权限管理安全以及其他访问控制措施的安全
35			未加限制的外部可访问锁	宜对外部可访问锁加以限制, 不允许被预期范围之外的实体影响
36	日志安全	对输出日志中特殊元素处理		应对输出日志中的特殊元素进行过滤和验证
37		信息丢失或遗漏		宜避免安全相关信息丢失或遗漏

二、代码实现安全缺陷审计（25 条审计条款）

序号	审计项/审计条款		审计指标
1	面向对象程序安全	泛型和非泛型数据类型	不宜混用具有泛型和非泛型的数据类型
2		包含敏感信息类的安全	包含敏感信息的类不应可复制和可序列化
3		类比较	在类进行比较时, 不宜只使用名称比较

4		类私有可变成员的引用	应禁止返回类的私有可变成员的引用
5		存储不可序列化的对象到磁盘	不应将不可序列化的对象存储到磁盘
6	并发程序安全	不同会话间信息泄露	代码应避免不同会话之间发生信息泄露
7		发布未完成初始化的对象	不宜发布未完成初始化的对象
8		共享资源的并发安全	共享资源宜使用正确的并发处理机制
9		子进程访问父进程敏感资源	在调用子进程之前应关闭敏感文件描述符，避免子进程使用这些描述符来执行未经授权的 I/O 操作
10		释放线程专有对象	应及时释放线程专有对象
11	函数调用安全	格式化字符串	应避免外部控制的格式化字符串
12		对方法或函数参数验证	宜对方法或函数的参数进行验证
13		参数指定错误	函数功能调用宜正确指定参数
14		返回栈变量地址	不宜返回栈变量地址
15		实现不一致函数	不宜使用具有不一致性实现的函数或方法
16		暴露危险的方法或函数	不应暴露危险的方法或函数
17	异常处理安全		宜恰当进行异常处理
18	指针安全	不兼容的指针类型	不宜使用不兼容类型的指针来访问变量
19		利用指针减法确定内存大小	宜避免使用指针的减法来确定内存大小
20		将固定地址赋值给指针	不宜把固定地址赋值给指针
21		试图访问非结构体类型指针的数据域	不应把指向非结构体类型指针强制转换为指向结构类型的指针并访问其字段
22		指针偏移越界	不应使用偏移越界的指针
23		无效指针使用	应避免无效指针的使用
24	代码生成安全	编译环境安全	应构建安全的编译环境
25		链接环境安全	应构建安全的链接环境

三、资源使用安全缺陷审计（32 条审计条款）

序号	审计项/审计条款	审计指标
1	资源管理	重复释放资源
2		应避免重复释放资源
3		资源或变量不安全初始化
4		初始化失败后未安全退出
5		应避免不安全的资源或变量初始化
6		初始化失败后应安全退出程序
7		引用计数的更新不正确
8		应避免引用计数的更新不正确
9		资源不安全清理
10	资源管理	宜避免不安全的资源清理
11		将资源暴露给非授权范围
12	资源管理	不应将资源暴露给非授权的范围
13		未经控制的递归
14	资源管理	应避免未经控制的递归
15		无限循环
16	资源管理	执行迭代或循环应恰当地限制循环执行的次数，以避免无限循环
17		算法复杂度攻击
18	资源管理	宜避免算法复杂度攻击

10		早期放大攻击	宜遵守正确的行为次序避免早期放大攻击数据
11	内存管理	内存分配释放函数成对调用	应成对调用内存分配和释放函数
12		堆内存释放	应避免在释放堆内存前清理不恰当而导致敏感信息暴露
13		内存未释放	宜及时释放动态分配的内存
14		访问已释放内存	不应引用或访问已被释放后的内存
15		数据/内存布局	不宜依赖数据/内存布局
16		内存缓冲区边界操作	应避免内存缓冲区边界操作发生越界
17		缓冲区复制造成溢出	应避免未检查输入数据大小就进行缓冲区复制
18		使用错误长度访问缓冲区	应避免使用错误的长度值访问缓冲区
19		堆空间耗尽	应限制堆空间的消耗, 防止堆空间耗尽
20	数据库使用	及时释放数据库资源	宜及时释放数据库资源
21		SQL 注入	应正确处理 SQL 命令中的特殊元素
22	文件管理	过期的文件描述符	不应使用过期的文件描述符
23		不安全的临时文件	应安全使用临时文件
24		文件描述符穷尽	不宜导致文件描述符穷尽
25		路径遍历	应避免路径遍历
26		及时释放文件系统资源	应及时释放文件系统资源
27	网络传输	端口多重绑定	不应在同一端口进行多重绑定
28		对网络消息容量的控制	宜避免对网络消息容量的控制不充分
29		字节序使用	应避免字节序使用不一致性
30		通信安全	应采用加密传输方式保护敏感数据
31		会话过期机制缺失	宜制定会话过期机制
32		会话标识符	宜确保会话标识符的随机性

四、环境安全安全缺陷审计（3 条审计条款）

序号	审计项/审计条款	审计指标
1	遗留调试代码	代码中不应遗留调试代码
2	第三方软件安全可靠	应对第三方代码来源情况进行审计, 确保引入的第三方软件安全可靠
3	保护重要配置信息	宜对重要的配置信息进行安全保护

6.1.1.6 测试结果概述

信息安全性—代码审计, 测试结果 见下表。

信息安全性—代码审计测试结果

审计条款总数量	97
审计条款符合数量	97
审计条款不符合数量	0

安全缺陷审计结果:

一、安全功能缺陷审计（37 条审计条款）

序号	审计项/审计条款			审计指标	审计结果
1	数据清洗	输入验证	关键状态数据外部可控	应避免关键状态数据被外部控制	符合
2			数据真实性验证	宜验证数据真实性，避免接收无效数据	符合
3			绕过数据净化和验证	宜防止以大小写混合的方式绕过数据净化和验证	符合
4			在字符串验证前未进行过滤	不宜在过滤字符串之前对字符串进行验证	符合
5			对 HTTP 头 Web 脚本特殊元素处理	应对 HTTP 头的 Web 脚本语法中的特殊元素进行过滤和验证	符合
6			命令行注入	应正确处理命令中的特殊元素	符合
7			数据结构控制域安全	宜避免对数据结构控制域的删除或意外增加。	符合
8			忽略字符串结尾符	应保证字符串的存储具有足够的空间容纳字符数据和结尾符	符合
9			对环境变量长度做出假设	不应对环境变量的长度做出假设	符合
10			条件比较不充分	执行比较时不应部分比较或不充分的比较	符合
11			结构体长度	不应将结构体的长度等同于其各个成员长度之和	符合
12			数值赋值越界	应避免数值赋值越界	符合
13			除零错误	应避免除零错误	符合
14			边界值检查缺失	数值范围比较时，不宜遗漏边界值检查	符合
15			数据信任边界的违背	代码应避免将可信和不可信数据组合在同一结构体中，违背信任边界	符合
16			条件语句缺失默认情况	条件语句中不宜缺失默认情况	符合
17			无法执行的死代码	不宜包含无法执行的死代码	符合
18			表达式永真或永假	不应出现表达式永真或永假代码	符合
19		输出编码	跨站脚本	应避免跨站脚本攻击	符合
20			Web 应用重定向后执行额外代码	Web 应用不宜在重定向后执行额外代码	符合
21			URL 重定向	不应开放不可信站点的 URL 重定向	符合
22	数据加密与保护	数据加密	密码安全	密码相关实现技术应符合国家密码相关管理规定	符合

23			随机数安全	应确保产生安全的随机数	符合
24			使用安全相关的硬编码	不应使用安全相关的硬编码	符合
25		数据保护	敏感信息暴露	应避免敏感信息暴露	符合
26			个人信息保护	应确保个人信息保护	符合
27	访问控制	身份鉴别	身份鉴别过程中暴露多余信息	应避免在处理身份鉴别的过程中暴露多余信息	符合
28			身份鉴别被绕过	应避免身份鉴别被绕过	符合
29			身份鉴别尝试频率限制	应对身份鉴别连续多次登录失败频率进行限制	符合
30			多因素认证	宜使用多因素认证机制	符合
31		口令安全	登录口令	应确保登录过程中口令不可明文显示	符合
32			明文存储口令	应避免明文存储口令	符合
33			明文传递口令	应避免明文传递口令	符合
34		权限管理	权限访问控制	应确保权限管理安全以及其他访问控制措施的安全	符合
35			未加限制的外部可访问锁	宜对外部可访问锁加以限制，不允许被预期范围之外的实体影响	符合
36	日志安全	对输出日志中特殊元素处理		应对输出日志中的特殊元素进行过滤和验证	符合
37		信息丢失或遗漏		宜避免安全相关信息丢失或遗漏	符合

二、代码实现安全缺陷审计（25 条审计条款）

序号	审计项/审计条款		审计指标	审计结果
1	面向对象程序安全	泛型和非泛型数据类型	不宜混用具有泛型和非泛型的数据类型	符合
2		包含敏感信息类的安全	包含敏感信息的类不应可复制和可序列化	符合
3		类比较	在类进行比较时，不宜只使用名称比较	符合
4		类私有可变成员的引用	应禁止返回类的私有可变成员的引用	符合
5		存储不可序列化的对象到磁盘	不应将不可序列化的对象存储到磁盘	符合
6	并发程序安全	不同会话间信息泄露	代码应避免不同会话之间发生信息泄露	符合
7		发布未完成初始化的对象	不宜发布未完成初始化的对象	符合
8		共享资源的并发安全	共享资源宜使用正确的并发处理机制	符合

9		子进程访问父进程敏感资源	在调用子进程之前应关闭敏感文件描述符，避免子进程使用这些描述符来执行未经授权的 I/O 操作	符合
10		释放线程专有对象	应及时释放线程专有对象	符合
11	函数调用安全	格式化字符串	应避免外部控制的格式化字符串	符合
12		对方法或函数参数验证	宜对方法或函数的参数进行验证	符合
13		参数指定错误	函数功能调用宜正确指定参数	符合
14		返回栈变量地址	不宜返回栈变量地址	符合
15		实现不一致函数	不宜使用具有不一致性实现的函数或方法	符合
16		暴露危险的方法或函数	不应暴露危险的方法或函数	符合
17	异常处理安全		宜恰当进行异常处理	符合
18	指针安全	不兼容的指针类型	不宜使用不兼容类型的指针来访问变量	符合
19		利用指针减法确定内存大小	宜避免使用指针的减法来确定内存大小	符合
20		将固定地址赋值给指针	不宜把固定地址赋值给指针	符合
21		试图访问非结构体类型指针的数据域	不应把指向非结构体类型指针强制转换为指向结构类型的指针并访问其字段	符合
22		指针偏移越界	不应使用偏移越界的指针	符合
23		无效指针使用	应避免无效指针的使用	符合
24	代码生成安全	编译环境安全	应构建安全的编译环境	符合
25		链接环境安全	应构建安全的链接环境	符合

三、资源使用安全缺陷审计（32 条审计条款）

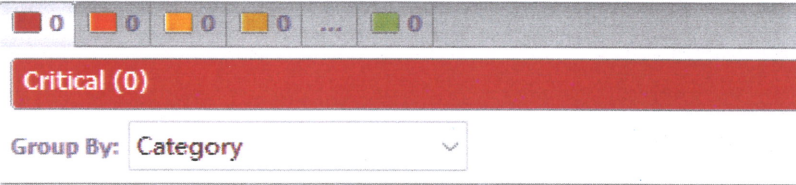
序号	审计项/审计条款		审计指标	审计结果
1	资源管理	重复释放资源	应避免重复释放资源	符合
2		资源或变量不安全初始化	宜避免不安全的资源或变量初始化	符合
3		初始化失败后未安全退出	初始化失败后应安全退出程序	符合
4		引用计数的更新不正确	应避免引用计数的更新不正确	符合
5		资源不安全清理	宜避免不安全的资源清理	符合
6		将资源暴露给非授权范围	不应将资源暴露给非授权的范围	符合
7		未经控制的递归	应避免未经控制的递归	符合

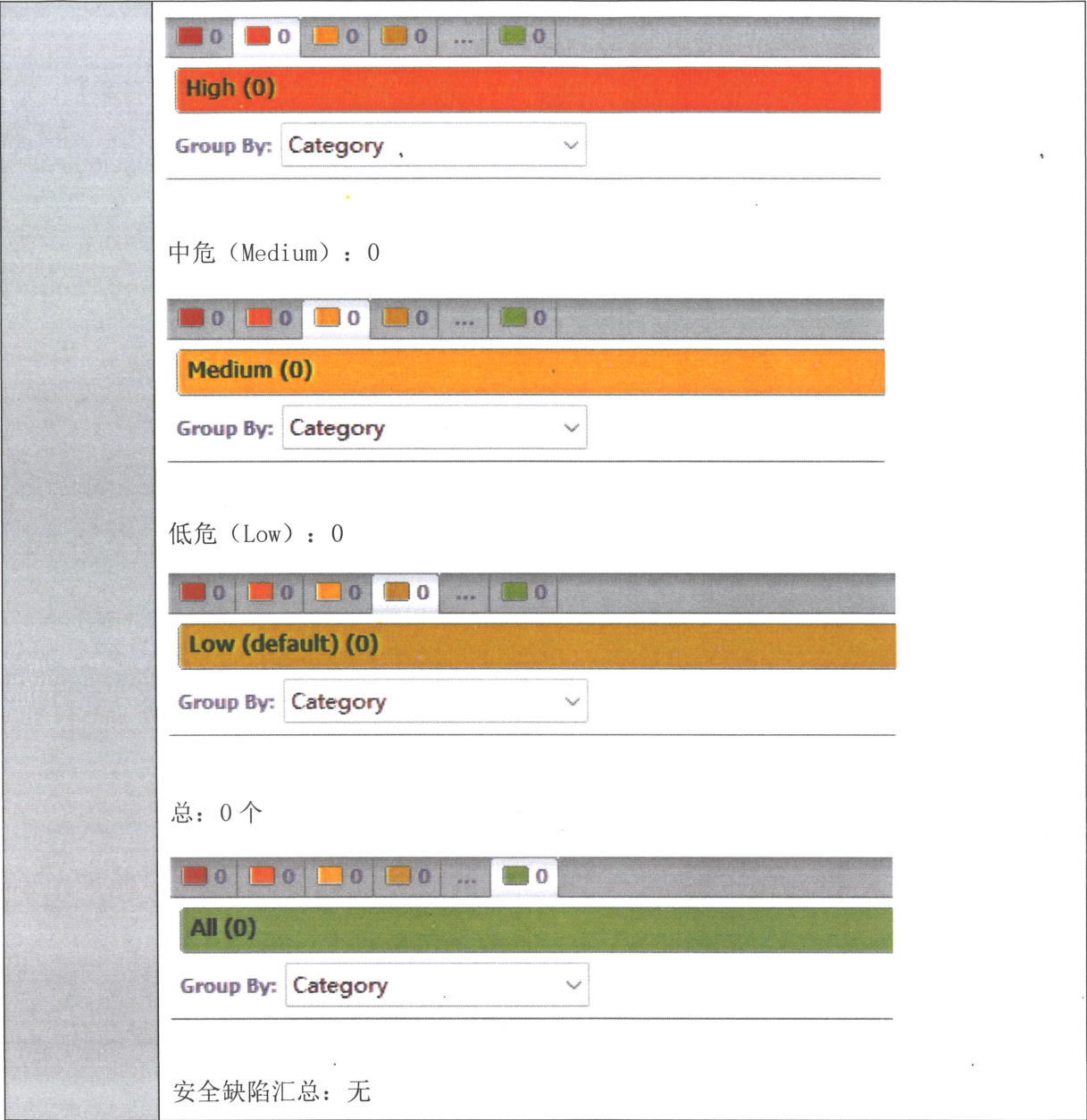
8		无限循环	执行迭代或循环应恰当地限制循环执行的次数，以避免无限循环	符合
9		算法复杂度攻击	宜避免算法复杂度攻击	符合
10		早期放大攻击	宜遵守正确的行为次序避免早期放大攻击数据	符合
11	内存管理	内存分配释放函数成对调用	应成对调用内存分配和释放函数	符合
12		堆内存释放	应避免在释放堆内存前清理不恰当而导致敏感信息暴露	符合
13		内存未释放	宜及时释放动态分配的内存	符合
14		访问已释放内存	不应引用或访问已被释放后的内存	符合
15		数据/内存布局	不宜依赖数据/内存布局	符合
16		内存缓冲区边界操作	应避免内存缓冲区边界操作发生越界	符合
17		缓冲区复制造成溢出	应避免未检查输入数据大小就进行缓冲区复制	符合
18		使用错误长度访问缓冲区	应避免使用错误的长度值访问缓冲区	符合
19		堆空间耗尽	应限制堆空间的消耗，防止堆空间耗尽	符合
20	数据库使用	及时释放数据库资源	宜及时释放数据库资源	符合
21		SQL 注入	应正确处理 SQL 命令中的特殊元素	符合
22	文件管理	过期的文件描述符	不应使用过期的文件描述符	符合
23		不安全的临时文件	应安全使用临时文件	符合
24		文件描述符穷尽	不宜导致文件描述符穷尽	符合
25		路径遍历	应避免路径遍历	符合
26		及时释放文件系统资源	应及时释放文件系统资源	符合
27	网络传输	端口多重绑定	不对同一端口进行多重绑定	符合
28		对网络消息容量的控制	宜避免对网络消息容量的控制不充分	符合
29		字节序使用	应避免字节序使用不一致性	符合
30		通信安全	应采用加密传输方式保护敏感数据	符合
31		会话过期机制缺失	宜制定会话过期机制	符合
32		会话标识符	宜确保会话标识符的随机性	符合

四、环境安全安全缺陷审计（3 条审计条款）

序号	审计项/审计条款	审计指标	审计结果
1	遗留调试代码	代码中不应遗留调试代码	符合
2	第三方软件安全可靠	应对第三方代码来源情况进行审计，确保引入的第三方软件安全可靠	符合
3	保护重要配置信息	宜对重要的配置信息进行安全保护	符合

6.1.1.7 测试结果分析

用例集名称	代码安全审计			用例集标识	——
测试项名称	安全漏洞检查及审计			测试项标识	——
测试版本	V1.0			用例设计方法	错误猜测/缺陷验证
评估准则	测试的实际结果与预期结果一致，则用例通过。				
用例描述	通过代码审计工具对目标代码进行安全漏洞检查，查找紧危风险、高危风险和中危风险以上安全风险问题，并针对发现的漏洞进行审计				
初始化	被测件正常运行				
前提和约束	/				
测试步骤	1. 通过代码审计工具对目标代码进行安全漏洞检查，查找紧危风险、高危风险和中危风险以上安全风险问题； 2. 针对发现的漏洞进行审计。				
预期结果	未发现紧危风险、高危风险和中危风险以上安全风险问题，所发现的安全问题可控。				
测试结果	测试阶段	测试人员/时间	监督人员/时间	测试情况	测试结论
	首轮测试	郑凯亮 /2026.08.12	王小宙 /2026.08.12	未发现紧危风险、高危风险和中危风险以上安全风险问题，所发现的安全问题可控。	通过
首轮测试结果及截图	未发现紧危风险、高危风险和中危风险以上安全风险问题。 检测结果：共 0 个漏洞问题，无可执行利用中高危漏洞。 超危/紧危 (Critical) : 0  高危 (High) : 0				



—————报告结束—————

本报告已经过区块链技术全流程上链存证和保护



报告查询码: 2be68dac

区块链证书验真请扫描上述二维码或直接官网输入报告查询码进行查询验证

