报告编号：SYDZ233SA1TP

检 测 报 告

项目名称：漏洞扫描

委托单位：大族激光科技产业集团股份有限公司

系统名称：卷烟二维码统一应用系统（V2.0）

银行卡检测中心

北京银联金卡科技有限公司

中国北京市石景山区实兴大街 30 号院 18 号楼

电话：86-10-81131728 传真：86-10-81131500 网址：www.bctest.com

声 明

本报告的评估结果仅对评估时间段内信息系统的现状有效，评估后系统出现任何变更，本报告结果不再适用。

考虑到评估工作的时间、范围限制，以及测试技术的局限性，信息系统可能仍存在未发现的安全风险。

本报告为严格保密，除大族激光科技产业集团股份有限公司外，此报告不应分发给没有得到认可的第三方，或被没有得到认可的第三方引用。

注意事项：

1. 报告无银行卡检测中心公章无效。
2. 报告未经银行卡检测中心批准，不得部分复制。
3. 测试结果一律以检测报告为准。
4. 报告无批准人员的签字无效。
5. 报告涂改无效。
6. 本报告的最终解释权归银行卡检测中心所有。

目 录

报 告 摘 要

2023 年 11 月 6 日至 2023 年 11 月 10 日，受大族激光科技产业集团股份有限公司（以下简称“大族激光”）委托，银行卡检测中心（下文简称“中心”）依据《金融网络安全 Web 应用服务安全测试通用规范》（JR/T 0213-2021）对大族激光科技产业集团股份有限公司的卷烟二维码统一应用系统（V2.0）包含：“盒条件”关联厂级管理子系统（V2.0）、“条零”关联物流中心级管理子系统（V2.0）、“盒条”关联现场管理子系统（V2.0）、“条件”关联现场管理子系统（V2.0）、“盒条”关联人工作业单元（V2.0）、“条件”关联人工作业单元（V2.0）、“条零”关联现场管理子系统（V2.0）、“盒条件”关联人工作业单元 apk、“条零”关联人工作业单元 apk 进行了漏洞扫描。本报告分为以下六个部分：测试基本信息、测试环境和测试过程简介、漏洞扫描结果综述、漏洞扫描检测点、漏洞发现详情、漏洞扫描结论与建议。

通过漏洞扫描发现大族激光科技产业集团股份有限公司的“盒条件”关联人工作业单元 apk、“条零”关联人工作业单元 apk 存在安全漏洞如下：

高危问题：1 个；

中危问题：2 个；

低危问题：3 个；

经复测验证，确认其中 1 个高危问题、2 个中危问题、1 个低危问题已经得到解决。

报告有效期为一年。

检测：张杰 复核：谷雨 批准：高祖康

银行卡检测中心

二〇二三年十一月二十二日

一、 测试基本信息

委托单位信息	单位名称	大族激光科技产业集团股份有限公司		
	联系人	颜彬彬		
	联系电话	18868949453		
	E-MAIL	1037269602@qq.com		
	联系地址	/		
测试时间	2023 年 11 月 6 日至 2023 年 11 月 10 日 测试时间段：9:30 至 17:30			
测试单位	☐ 内部测试 ■ 外部服务机构测试：银行卡检测中心			
测试团队	姓名	张杰	单位	银行卡检测中心
	岗位角色	安全评估工程师	联系方式	zhangjie@bctest.com
测试地址及账号	卷烟二维码统一应用系统（V2.0）包含： “盒条件”关联厂级管理子系统测试环境 IP 地址： https://192.168. *.* “条零”关联物流中心级管理子系统测试环境 IP 地址： https://192.168. *.* “盒条”关联现场管理子系统（V2.0）测试环境 IP 地址： http://192.168. *.*:8086 “条件”关联现场管理子系统（V2.0）测试环境 IP 地址： http://192.168. *.*:8086			

	“盒条”关联人工作业单元（V2.0）测试环境 IP 地址： http://192.168. *.*:8086 “条件”关联人工作业单元（V2.0）测试环境 IP 地址： http://192.168. *.*:8086 “条零”关联现场管理子系统（V2.0）测试环境 IP 地址： http://192.168. *.*:8086 “盒条件”关联人工作业单元 apk： app-release-htj-1103.apk “条零”关联人工作业单元 apk： app-release-tl-1103.apk
测试目标	■ 限制目标 □ 不限制目标
测试 IP	192.168.*.*
系统环境	■ 测试环境 □ 生产环境

二、 测试环境和测试过程简介

(一) 参考标准

《金融网络安全 Web 应用服务安全测试通用规范》（JR/T 0213-2021）

《信息安全技术 信息安全风险评估规范》（GB/T 20984-2007）

《信息安全技术 术语》（GB/T 25069-2010）

《信息安全技术 信息安全风险评估实施指南》（GB/T 31509-2015）

《金融行业网络安全等级保护测评指南》（JR/T 0072-2020）

《网上银行系统信息安全通用规范》（JR/T 0068-2020）

(二) 测试原则

1. 标准性原则

按照 GB/T 31509-2015 和 JR/T 0072-2020 的流程进行实施，包括实施阶段和运维阶段的测试工作。

2. 全面性原则

在规定的测试范围内，应覆盖指定目标中的全部 Web 应用服务及每个 Web 应用服务中的全部功能。

3. 分级原则

测试过程中应对 Web 应用服务及漏洞进行分级管理，以保证重要 Web 应用服务的资源投入。

4. 可控性原则

测试过程应按照 GB/T 31509-2015 中的项目管理方法对过程、人员、工具等进行控制，以保证安全测试过程的安全可控。

5. 最小影响原则

针对处于运维阶段的 Web 应用服务，提前确定合适的测试时间窗口，避开业务高峰期，同时做好被测试目标应用服务的应急预案。

6. 保密性原则

未经被评估机构允许，测试方不应向第三方及社会公众泄露与安全测试目标相关的一切信息，包括但不限于开发及运维人员个人信息以及因测试活动所获取的敏感信息，如 Web 应用网络架构、业务数据、 安全漏洞等。

7. 及时性原则

测试方应保证漏洞提交的及时性，检测出漏洞与提交漏洞的时间间隔不应超出规定时间，不应出现漏洞积压的情况。

8. 局限性原则

测试方对同类型或同种类功能点进行测试时，由于同类型或同种类功能点的参数或者功能较多，需抽样 3～5 个进行测试，如：同类型商品提交及价格参数修改。后续需要被测方参照测试结果和过程开展相应测试工作。

(三) 测试环境及基本准备要求

1. 被评估机构应针对金融交易类应用提供与生产环境相似的仿真环境，以便进行部分可能影响数据完整性及业务稳定性的侵入式测试。测试方在生产环境中应避免使用可能导致数据完整性及业务稳定性遭受破坏的测试手段。

2. 被评估机构应预先准备功能与数据均完备的账号以保证测试的完备性，若完成测试涉及必要的专有设备，如控件、证书和 U 盾等软硬件设备，被评估机构应给予必要的配合或协助。

3. 如测试过程中发现功能损坏及数据缺失，测试方应对缺失的数据及损坏的功能进行详细记录，并及时反馈给系统开发人员进行功能及数据补足。

4. 通过仿真环境测试时，被评估机构应提供安全的测试接入方式，如现场接入、VPN 远程接入及 IP 白名单等方式，防止非授权人员对仿真环境进行违规访问或违规测试。

5. 禁止测试方向任何未经授权的第三方泄露与测试环境相关的任何信息。

6. 测试环境提供方应及时与测试方同步测试系统更新、维护及测试计划，以保证测试环境稳定可用。

7. 如测试目标为应用接口，测试环境提供方应向测试方提供足以用来构造并完成接口请求的说明文档或脚本。

(四) 测试工具信息

漏洞扫描人员模拟黑客入侵攻击的过程中使用的工具包含操作系统自带网络应用、管理和诊断工具、扫描器、远程入侵代码和本地提升权限代码以及测试人员自主开发的安全扫描工具。

测试工具基本信息：

工具名称	工具用途
Nessus	内网应用程序安全扫描系统。
绿盟远程安全评估系统	对常见的网络设备、操作系统、应用程序和数据库进行实时的、定时的扫描。
Fiddler	HTTP 数据包修改、转发工具。
Wireshark	Wireshark 是一个网络封包分析软件,功能是截取网络封包，并尽可能显示出最为详细的网络封包资料。
Nmap	Nmap 是一个网络连接端扫描软件，可以检测目标主机是否在线、端口开放情况、侦测运行的服务类型及版本信息、侦测操作系统与设备类型等信息。它是网络管理员必用的软件之一，用以评估网络系统安全。
Burp Suite	Burp Suite 是 web 应用程序漏洞扫描集成平台。其中包含了许多工具，并为这些工具设计了许多接口，以促进加快攻击应用程序的过程。平台中所有工具共享同一框架，以便统一处理 HTTP 请求、持久性、认证、上游代理、日志记录、报警和可扩展性。Burp Suite 允许攻击者结合手工和自动技术去枚举、分析、攻击 Web 应用程序。

SQLmap	Sqlmap 是一个自动化的 SQL 注入工具，其主要功能是扫描、发现并利用给定的 URL 的 SQL 注入漏洞，目前支持 MySQL、Oracle、PostgreSQL、Microsoft SQL Server、Microsoft Access 等主流数据库。
银行卡检测中心整理工具集	跨站及 SQL 注入测试、远程溢出测试、暴力破解测试、嗅探分析等。

表 1 测试工具基本信息表

(五) 测试流程

银行卡检测中心漏洞扫描服务流程定义为如下阶段：

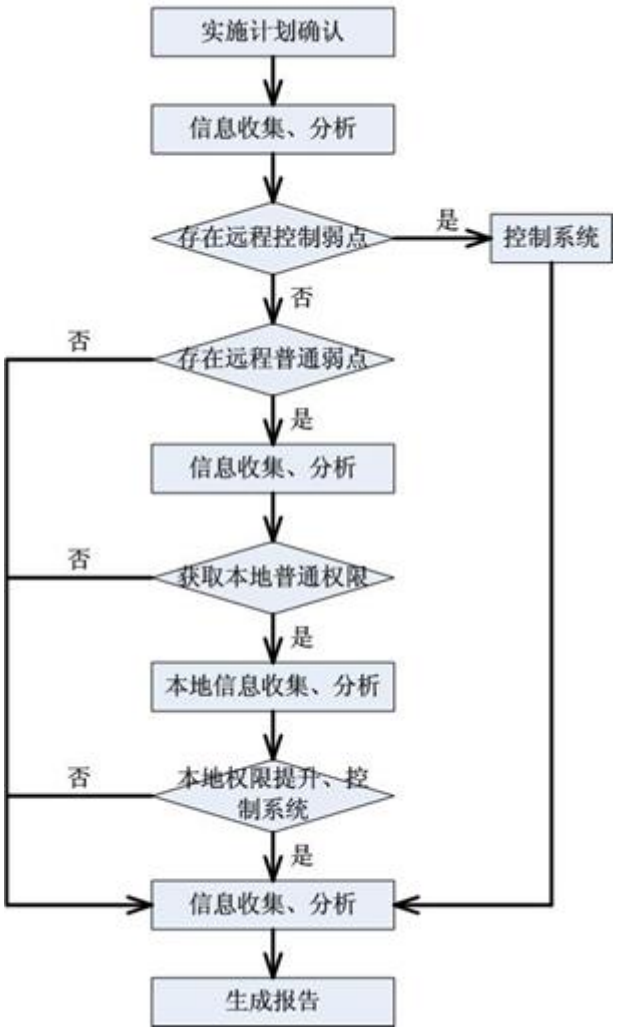


图 1 漏洞扫描流程图

信息收集：此阶段中，银行卡检测中心测试人员进行必要的信息收集，如真实 IP 地址、开放端口情况、DNS 记录、开发语言信息、开源框架或插件信息、软件版本信息、URL 路径信息、Google hacking 中的公开信息、安全防护情况等。

漏洞扫描：此阶段中，银行卡检测中心测试人员根据第一阶段获得的信息对网络、系统进行漏洞扫描。此阶段如果成功的话，可能获得普通权限。

缺陷利用：此阶段中，银行卡检测中心测试人员尝试由普通权限提升为管理员权限，获得对系统的完全控制权。在时间许可的情况下，必要时从第一阶段重新进行。

成果收集：此阶段中，银行卡检测中心测试人员对前期收集的各类弱点、漏洞等问题进行分类整理，集中展示。

威胁分析：此阶段中，银行卡检测中心测试人员对发现的上述问题进行威胁分类和分析其影响。

输出报告：此阶段中，银行卡检测中心测试人员根据测试和分析的结果编写直观的漏洞扫描服务报告。

(六) 术语定义

威胁程度分级：

高危（严重）：

- 存在重大问题，建议尽快改正。
- 与相关法律法规、标准规范有明显冲突；存在安全风险，会对客户利益造成严重的损害。

中危（一般）：

- 存在明显的问题，建议制定相应计划，在一定时期内改正。
- 存在安全风险，会对客户利益造成直接或潜在的损害。

低危（建议）：

此类风险一般不会直接危害系统安全性，但是如果版本更新或者软件的其它组件存在缺陷，可能成为新的风险点或者显著降低攻击者成功利用的难度。

三、 漏洞扫描结果综述

(一) “盒条件”关联厂级管理子系统 1

1. 测试结果汇总

本次银行卡检测中心对大族激光科技产业集团股份有限公司的“盒条件”关联厂级管理子系统（V2.0）进行漏洞扫描，共发现 0 个安全漏洞，其中高危 0 个、中危 0 个、低危 0 个，漏洞扫描安全漏洞汇总详见表 2。

测试项	修复前			修复后			修复前单测试项问题数量合计	修复后单测试项问题数量合计
	高危	中危	低危	高危	中危	低危		
业务逻辑	0	0	0	0	0	0	0	0
身份鉴别	0	0	0	0	0	0	0	0
授权	0	0	0	0	0	0	0	0
会话管理	0	0	0	0	0	0	0	0
输入验证	0	0	0	0	0	0	0	0
错误处理	0	0	0	0	0	0	0	0
密码学	0	0	0	0	0	0	0	0
Web客户端	0	0	0	0	0	0	0	0
敏感信息泄露	0	0	0	0	0	0	0	0
中间件	0	0	0	0	0	0	0	0
配置错误及框架漏洞	0	0	0	0	0	0	0	0
App客户端	0	0	0	0	0	0	0	0
总计	0	0	0	0	0	0	0	0

表 2 漏洞扫描安全漏洞汇总表

2. 漏洞问题清单

无。

(二)“条零”关联物流中心级管理子系统 2

1. 测试结果汇总

本次银行卡检测中心对大族激光科技产业集团股份有限公司的“条零”关联物流中心级管理子系统（V2.0）进行漏洞扫描，共发现 0 个安全漏洞，其中高危 0 个、中危 0 个、低危 0 个，漏洞扫描安全漏洞汇总详见表 2。

测试项	修复前			修复后			修复前单测试项问题数量合计	修复后单测试项问题数量合计
	高危	中危	低危	高危	中危	低危		
业务逻辑	0	0	0	0	0	0	0	0
身份鉴别	0	0	0	0	0	0	0	0
授权	0	0	0	0	0	0	0	0
会话管理	0	0	0	0	0	0	0	0
输入验证	0	0	0	0	0	0	0	0
错误处理	0	0	0	0	0	0	0	0
密码学	0	0	0	0	0	0	0	0
Web客户端	0	0	0	0	0	0	0	0
敏感信息泄露	0	0	0	0	0	0	0	0
中间件	0	0	0	0	0	0	0	0
配置错误及框架漏洞	0	0	0	0	0	0	0	0
App客户端	0	0	0	0	0	0	0	0
总计	0	0	0	0	0	0	0	0

表 32 漏洞扫描安全漏洞汇总表

2. 漏洞问题清单

无。

(三)“条零”关联现场管理子系统 3

1. 测试结果汇总

本次银行卡检测中心对大族激光科技产业集团股份有限公司的“条零”关联现场管理子系统（V2.0）进行漏洞扫描，共发现 0 个安全漏洞，其中高危 0 个、中危 0 个、低危 0 个，漏洞扫描安全漏洞汇总

详见表 2。

测试项	修复前			修复后			修复前单测试项问题数量合计	修复后单测试项问题数量合计
	高危	中危	低危	高危	中危	低危		
业务逻辑	0	0	0	0	0	0	0	0
身份鉴别	0	0	0	0	0	0	0	0
授权	0	0	0	0	0	0	0	0
会话管理	0	0	0	0	0	0	0	0
输入验证	0	0	0	0	0	0	0	0
错误处理	0	0	0	0	0	0	0	0
密码学	0	0	0	0	0	0	0	0
Web客户端	0	0	0	0	0	0	0	0
敏感信息泄露	0	0	0	0	0	0	0	0
中间件	0	0	0	0	0	0	0	0
配置错误及框架漏洞	0	0	0	0	0	0	0	0
App客户端	0	0	0	0	0	0	0	0
总计	0	0	0	0	0	0	0	0

表 ~~42~~ 漏洞扫描安全漏洞汇总表

2. 漏洞问题清单

无。

(四)“盒条”关联人工作业单元 4

1. 测试结果汇总

本次银行卡检测中心对大族激光科技产业集团股份有限公司的“盒条”关联人工作业单元（V2.0）进行漏洞扫描，共发现 0 个安全漏洞，其中高危 0 个、中危 0 个、低危 0 个，漏洞扫描安全漏洞汇总详见表 2。

测试项	修复前			修复后			修复前单测试项问题数量合计	修复后单测试项问题数量合计
	高危	中危	低危	高危	中危	低危		
业务逻辑	0	0	0	0	0	0	0	0
身份鉴别	0	0	0	0	0	0	0	0
授权	0	0	0	0	0	0	0	0
会话管理	0	0	0	0	0	0	0	0
输入验证	0	0	0	0	0	0	0	0
错误处理	0	0	0	0	0	0	0	0
密码学	0	0	0	0	0	0	0	0
Web客户端	0	0	0	0	0	0	0	0
敏感信息泄露	0	0	0	0	0	0	0	0
中间件	0	0	0	0	0	0	0	0
配置错误及框架漏洞	0	0	0	0	0	0	0	0
App客户端	0	0	0	0	0	0	0	0
总计	0	0	0	0	0	0	0	0

表 ~~52~~ 漏洞扫描安全漏洞汇总表

2. 漏洞问题清单

无。

(五)“盒条”关联现场管理子系统 5

1. 测试结果汇总

本次银行卡检测中心对大族激光科技产业集团股份有限公司的“盒条”关联现场管理子系统（V2.0）进行漏洞扫描，共发现 0 个安全漏洞，其中高危 0 个、中危 0 个、低危 0 个，漏洞扫描安全漏洞汇总详见表 2。

测试项	修复前			修复后			修复前单测试项问题数量合计	修复后单测试项问题数量合计
	高危	中危	低危	高危	中危	低危		
业务逻辑	0	0	0	0	0	0	0	0
身份鉴别	0	0	0	0	0	0	0	0
授权	0	0	0	0	0	0	0	0
会话管理	0	0	0	0	0	0	0	0
输入验证	0	0	0	0	0	0	0	0
错误处理	0	0	0	0	0	0	0	0
密码学	0	0	0	0	0	0	0	0
Web客户端	0	0	0	0	0	0	0	0
敏感信息泄露	0	0	0	0	0	0	0	0
中间件	0	0	0	0	0	0	0	0
配置错误及框架漏洞	0	0	0	0	0	0	0	0
App客户端	0	0	0	0	0	0	0	0
总计	0	0	0	0	0	0	0	0

表 62 漏洞扫描安全漏洞汇总表

2. 漏洞问题清单

无。

(六)“条件”关联人工作业单元 6

1. 测试结果汇总

本次银行卡检测中心对大族激光科技产业集团股份有限公司的“条件”关联人工作业单元（V2.0）进行漏洞扫描，共发现 0 个安全漏洞，其中高危 0 个、中危 0 个、低危 0 个，漏洞扫描安全漏洞汇总详见表 2。

测试项	修复前			修复后			修复前单测试项问题数量合计	修复后单测试项问题数量合计
	高危	中危	低危	高危	中危	低危		
业务逻辑	0	0	0	0	0	0	0	0
身份鉴别	0	0	0	0	0	0	0	0
授权	0	0	0	0	0	0	0	0
会话管理	0	0	0	0	0	0	0	0
输入验证	0	0	0	0	0	0	0	0
错误处理	0	0	0	0	0	0	0	0
密码学	0	0	0	0	0	0	0	0
Web客户端	0	0	0	0	0	0	0	0
敏感信息泄露	0	0	0	0	0	0	0	0
中间件	0	0	0	0	0	0	0	0
配置错误及框架漏洞	0	0	0	0	0	0	0	0
App客户端	0	0	0	0	0	0	0	0
总计	0	0	0	0	0	0	0	0

表 72 漏洞扫描安全漏洞汇总表

2. 漏洞问题清单

无。

(七)“条件”关联现场管理子系统 7

1. 测试结果汇总

本次银行卡检测中心对大族激光科技产业集团股份有限公司的

“条件”关联现场管理子系统（V2.0）进行漏洞扫描，共发现 0 个安全漏洞，其中高危 0 个、中危 0 个、低危 0 个，漏洞扫描安全漏洞汇总详见表 2。

测试项	修复前			修复后			修复前单测试项问题数量合计	修复后单测试项问题数量合计
	高危	中危	低危	高危	中危	低危		
业务逻辑	0	0	0	0	0	0	0	0
身份鉴别	0	0	0	0	0	0	0	0
授权	0	0	0	0	0	0	0	0
会话管理	0	0	0	0	0	0	0	0
输入验证	0	0	0	0	0	0	0	0
错误处理	0	0	0	0	0	0	0	0
密码学	0	0	0	0	0	0	0	0
Web客户端	0	0	0	0	0	0	0	0
敏感信息泄露	0	0	0	0	0	0	0	0
中间件	0	0	0	0	0	0	0	0
配置错误及框架漏洞	0	0	0	0	0	0	0	0
App客户端	0	0	0	0	0	0	0	0
总计	0	0	0	0	0	0	0	0

表 ~~82~~ 漏洞扫描安全漏洞汇总表

2. 漏洞问题清单

无。

（八）“盒条件”关联人工作业单元 apk 8

1. 测试结果汇总

本次银行卡检测中心对大族激光科技产业集团股份有限公司的“盒条件”关联人工作业单元 apk 进行漏洞扫描，共发现 6 个安全漏洞，其中高危 1 个、中危 2 个、低危 3 个。漏洞扫描安全漏洞汇总详见表 2，安全漏洞分布情况详见图 2 和图 3。

测试项	修复前			修复后			修复前单测试项问题数量合计	修复后单测试项问题数量合计
	高危	中危	低危	高危	中危	低危		
业务逻辑	0	0	0	0	0	0	0	0
身份鉴别	0	1	0	0	0	0	1	0
授权	0	1	2	0	0	1	3	1
会话管理	0	0	0	0	0	0	0	0
输入验证	0	0	1	0	0	1	1	1
错误处理	0	0	0	0	0	0	0	0
密码学	0	0	0	0	0	0	0	0
Web客户端	0	0	0	0	0	0	0	0
敏感信息泄露	1	0	0	0	0	0	1	0
中间件	0	0	0	0	0	0	0	0
配置错误及框架漏洞	0	0	0	0	0	0	0	0
App客户端	0	0	0	0	0	0	0	0
总计	1	2	3	0	0	2	6	2

表 92 漏洞扫描安全漏洞汇总表

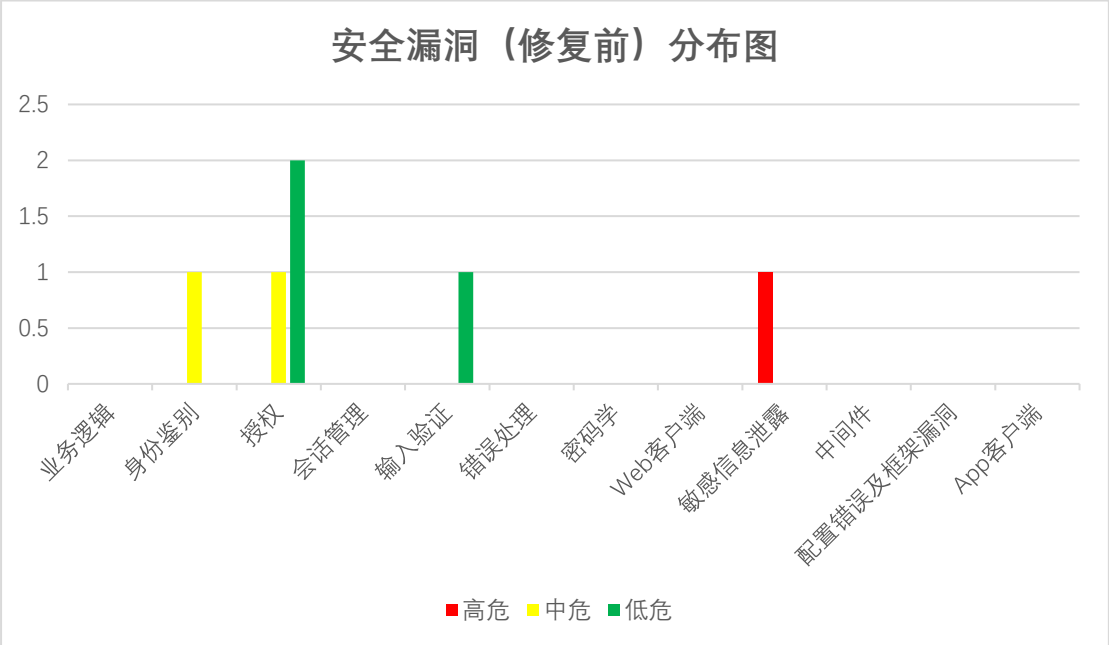


图 2 安全漏洞（修复前）分布图

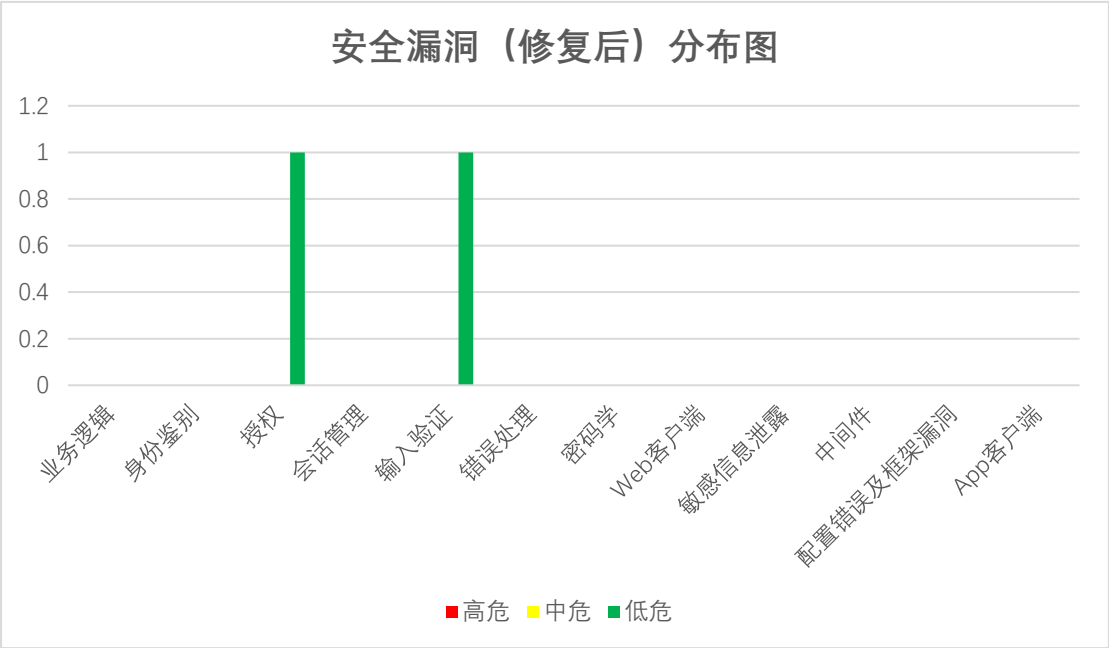


图 3 安全漏洞（修复后）分布图

2. 漏洞问题清单

序号	系统名称	漏洞等级	漏洞编号	漏洞名称	修复状态
1	“盒条件”关联人工作业单元	高危	9.1	敏感信息泄露	已修复
2		中危	2.7	认证绕过	已修复
3			3.6	不安全的直接对象引用	已修复
4		低危	3.2	目录浏览	已修复
5			5.1	XSS跨站脚本攻击	未修复
6			3.1	目录遍历	未修复

(九)“条零”关联人工作业单元 apk 9

1. 测试结果汇总

本次银行卡检测中心对大族激光科技产业集团股份有限公司的“条零”关联人工作业单元 apk 进行漏洞扫描，共发现 6 个安全漏洞，其中高危 1 个、中危 2 个、低危 3 个。漏洞扫描安全漏洞汇总详见表 2，安全漏洞分布情况详见图 2 和图 3。

测试项	修复前			修复后			修复前单测试项问题数量合计	修复后单测试项问题数量合计
	高危	中危	低危	高危	中危	低危		
业务逻辑	0	0	0	0	0	0	0	0
身份鉴别	0	1	0	0	0	0	1	0
授权	0	1	2	0	0	1	3	1
会话管理	0	0	0	0	0	0	0	0
输入验证	0	0	1	0	0	1	1	1
错误处理	0	0	0	0	0	0	0	0
密码学	0	0	0	0	0	0	0	0
Web客户端	0	0	0	0	0	0	0	0
敏感信息泄露	1	0	0	0	0	0	1	0
中间件	0	0	0	0	0	0	0	0
配置错误及框架漏洞	0	0	0	0	0	0	0	0
App客户端	0	0	0	0	0	0	0	0
总计	1	2	3	0	0	2	6	2

表 10~~2~~ 漏洞扫描安全漏洞汇总表

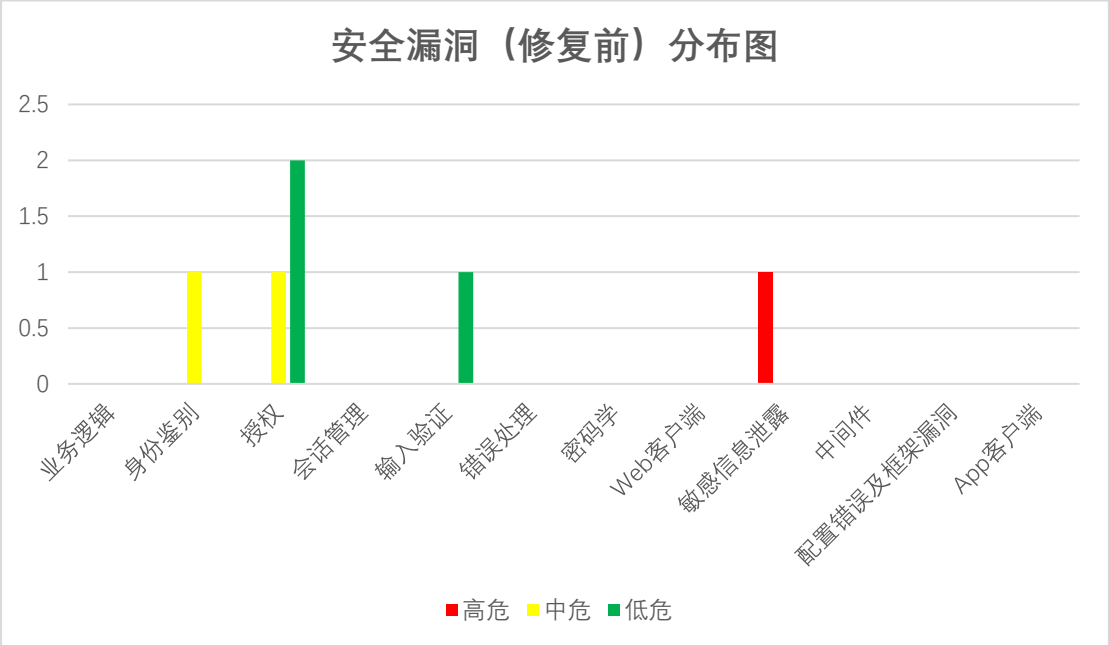


图 2 安全漏洞（修复前）分布图

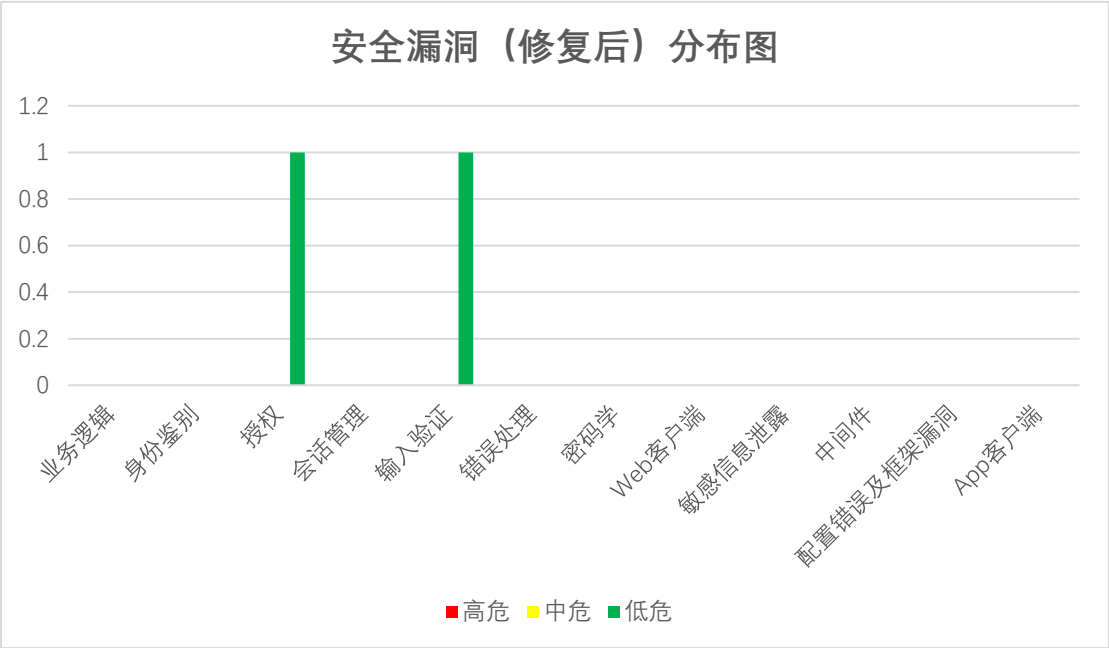


图 3 安全漏洞（修复后）分布图

2. 漏洞问题清单

序号	系统名称	漏洞等级	漏洞编号	漏洞名称	修复状态
1	“条零”关联人工作业单元	高危	9.1	敏感信息泄露	已修复
2		中危	2.7	认证绕过	已修复
3			3.6	不安全的直接对象引用	已修复
4		低危	3.2	目录浏览	已修复
5			5.1	XSS跨站脚本攻击	未修复
6			3.1	目录遍历	未修复

四、 漏洞测试检测点

(一) 业务逻辑测试

编号	1.1	测试点	多线程竞争条件	测试情况
测试内容及要求	1.在仿真环境中进行涉及资金交易的多线程竞争条件测试。通过对比分析判断生产环境中是否存在类似问题。 2.应至少覆盖转账及积分兑换等场景。			■已测试 □不具备测试条件 □不适用
编号	**1.2**	**测试点**	**资金查询越权**	**测试情况**

测试内容及要求	1.通过测试确认指定账户查询的回显内容中不包含当前用户权限所无法查看的内容。 2.测试覆盖到每一个可能对当前用户权限产生影响的参数。			■已测试 □不具备测试条件 □不适用
编号	**1.3**	**测试点**	**资金交易越权**	**测试情况**
测试内容及要求	1.测试确认不存在同一机构不同账户之间混淆的情况，如将预付账户资金直接汇入应付账户并完成虚假交易。 2.测试确认不同机构之间不存在平行越权问题，如测试方利用漏洞诱导他人完成自己账户的支付。			■已测试 □不具备测试条件 □不适用
编号	**1.4**	**测试点**	**支付漏洞**	**测试情况**
测试内容及要求	1.在仿真环境中进行支付漏洞测试。通过对比分析判断生产环境中是否存在类似问题。 2.订单提交前进行金额篡改提交；订单提交后进行支付时进行金额篡改提交。 3.确认商品属性篡改问题，商品属性包括但不限于商品金额、商品有效期、增值服务有效期、商品分期数和附加优惠等。 4.确认支付功能不存在 0 元支付问题，如删除金额参数或将金额参数置为 0 可以生成合法订单。 5.确认支付功能不存在整数溢出问题。 6.确认支付功能不存在负值反充问题，如通过支付负数成功导致账户余额增加。 7.确认支付功能不存在正负值对冲问题，如在进行多个不同类型商品结算支付时，可以通过正负值对冲构造低价订单。 8.确认支付功能不存在流程异常的问题，如输入非法的金额或数量导致应用出现异常或跳转至预期之外的流程。 9.确认支付功能不存在线程并发漏洞，导致商品价格由于并发改变，导致存在低价订单。			■已测试 □不具备测试条件 □不适用
编号	**1.5**	**测试点**	**请求重放**	**测试情况**
测试内容及要求	应通过测试确认任何涉及资金交易、数据修改、发送短信的操作均无法通过重放数据包的方式被重复执行。			■已测试 □不具备测试条件 □不适用
编号	**1.6**	**测试点**	**用户信息完整性**	**测试情况**
测试内容及要求	1.应用强制要求用户进行实名认证的场景，应通过测试确认用户在漏填实名认证信息的情况下不能完成注册。实名认证关键信息包括但不限于银行卡四要素、身份证四要素以及生物特征要素等。 2.通过测试确认用户在漏填账户关键信息的情况下不能完成注册。账户关键信息包括但不限于用户名、密码、手机号码、电子邮箱、密保问题等信息。			■已测试 □不具备测试条件 □不适用

	3.通过测试确认用户在操作大额交易或找回密码时，无法通过未进行设置的账户关键信息完成客户身份检查。如账户未设置密保问题的情况下，可以通过将密保问题参数置空绕过校验。 4.通过整体提交，查看不同响应回显状态码，是否可以绕过用户信息完整性的提交。			
编号	**1.7**	**测试点**	**业务逻辑数据验证**	**测试情况**
测试内容及要求	通过测试确认其他不涉及资金支付的业务逻辑功能不存在数据验证缺陷。如将相关业务逻辑功能中的各个关键参数赋值为空值、0 值、负数、超大数、字符串、换行符或制表符，以及将相关参数键值对整体删除之后出现的各类非预期结果。			■已测试 □不具备测试条件 □不适用
编号	**1.8**	**测试点**	**隐藏域**	**测试情况**
测试内容及要求	1.充分发现并记录隐藏域中的参数，并尝试对这些参数进行直接赋值以模拟非预期的请求。如在隐藏域中发现参数 admin，尝试直接在请求中增加 admin=1 后立即获得管理员权限。 2.结合业务语境充分猜测可能的隐藏参数，并尝试对这些参数进行直接赋值以模拟非预期的请求。如猜测会存在参数 admin，尝试直接在请求中增加 admin=1 后立即获得管理员权限。			■已测试 □不具备测试条件 □不适用
编号	**1.9**	**测试点**	**完整性检查和中间人**	**测试情况**
测试内容及要求	1.通过测试确认客户端和服务器在传输交易数据时，服务端采用了有效的完整性检查和防篡改措施。 2.通过测试确认客户端和服务器之间进行双向认证的有效性，确保无法通过已知手段进行中间人攻击。			■已测试 □不具备测试条件 □不适用
编号	**1.10**	**测试点**	**短信和电子邮箱验证**	**测试情况**
测试内容及要求	1.通过测试确认短信和电子邮箱验证逻辑不会被整体绕过。 2.通过测试确认短信和电子邮箱验证功能不存在短信和电子邮箱验证码前端生成问题。 3.应通过测试确认短信和电子邮箱验证功能不存在短信和电子邮箱验证码前端验证问题，如修改短信回显状态值绕过校验。 4.对于生产环境，通过测试确认短信和电子邮箱验证功能不存在短信和电子邮箱验证码前端验证问题，邮箱验证功能不存在特权验证码。 5.通过测试确认短信和电子邮箱验证功能存在有效的抗暴力破解措施。 6.通过测试确认短信和电子邮箱验证码的随机性，并确认短信和电子邮箱验证码的长度不少于 6 位数。 7.通过测试确认短信和电子邮箱验证码的失效时间不长于 6 分钟，并确保验证码到期后立即作废。 8.通过测试确认短信验证功能不存在内容定制的问题。如通过			■已测试 □不具备测试条件 □不适用

	参数插入任意文本拼接到短信内容中，防止出现钓鱼诱导短信。 9.通过测试确认短信和电子邮箱验证功能不存在定向转发漏洞，如可将当前用户的验证码或身份验证链接通过指定手机号码的方式定向转发至其他手机号码或电子邮箱上。 10.通过测试确认短信、邮件验证码是否可以被复用，如密码修改处的短信验证码可以用来交易等。 11.通过测试确认短信验证功能不存在短信重放的问题。如可向指定手机号码批量定向发送短信或批量向任意手机号码发送短信 10 次以上。 12.通过测试确认短信验证码或邮件验证码是否在响应包中进行回显，导致信息泄露。			
编号	**1.11**	**测试点**	**图形验证码**	**测试情况**
测试内容及要求	1.通过测试确认图形验证码不会被整体绕过。 2.通过测试确认图形验证码无法进行低成本的光学字符识别（OCR）。如互联网上可下载的 OCR 验证码识别工具、脚本等。 3.通过测试确认图形验证码认证 1 次后即刻失效。 4.通过抓包，看是否可以重复提交，验证码未及时刷新。			■已测试 □不具备测试条件 □不适用
编号	**1.12**	**测试点**	**滑块验证码**	**测试情况**
测试内容及要求	1.通过测试确认滑块验证码不会被整体绕过。 2.通过测试确认滑块验证码能够有效防止机器模拟验证。 3.通过测试确认滑块验证码认证 1 次后即刻失效。 4.通过抓包，看是否可以重复提交，验证码未及时刷新。			■已测试 □不具备测试条件 □不适用
编号	**1.13**	**测试点**	**处理用时**	**测试情况**
测试内容及要求	通过测试确认所有关键请求不能通过响应时间的变化而进行执行结果预测。如使用通配符导致的响应延迟可能是由于服务端使用了正则表达式，这种情况下攻击者可以通过调整输入以获得预期之外的最佳响应。			■已测试 □不具备测试条件 □不适用
编号	**1.14**	**测试点**	**工作流程绕过**	**测试情况**
测试内容及要求	1.至少在找回密码和重置密码场景处进行业务流程绕过测试。 2.通过测试确认当前所在的业务流程阶段不能够通过用户传入的参数直接指定。 3.对于每一个业务流程阶段，应通过测试确保安全策略与安全原则具备整体一致性。			■已测试 □不具备测试条件 □不适用
编号	**1.15**	**测试点**	**应用程序误用**	**测试情况**
测试内容及要求	通过测试确认系统存在能够阻止攻击者反复进行攻击尝试的防御机制。如多次输入疑似攻击尝试及攻击利用的内容，系统可以直接阻断请求并进行临时 IP 封禁。该机制可以由第三方设备			■已测试 □不具备测试条件

	或软件提供。			□不适用
编号	**1.16**	**测试点**	**文件上传**	**测试情况**
测试内容及要求	1.通过测试确认系统不存在可以直接部署网页脚本的文件上传功能。 2.通过测试确认存储上传文件的 Web 应用服务不存在脚本解析漏洞，如：00 截断等。 3.通过测试确认上传文档前应经过有效的身份验证。 4.通过测试确认文件上传的校验在服务端进行。 5.通过测试确认文件上传功能存在有效的后缀白名单限制，且无法被突破。 6.通过测试确认文件上传的位置无法通过参数进行指定或操控。 7.通过测试确认文件上传功能不存在竞争上传问题。 8.文件上传后会针对上传文件内容进行展示及重新渲染的功能，应通过测试确认无法利用该功能绕过现有防御机制。			■已测试 □不具备测试条件 □不适用
编号	**1.17**	**测试点**	**token 值校验**	**测试情况**
测试内容及要求	1.查看 token 的主要作用。 2.token 是否固定，每次是否一致。 3.token 传输方式是否使用 POST 请求。 4.token 是否被绕过。 5.token 的生成机制是否可以被猜测。			■已测试 □不具备测试条件 □不适用

(二) 身份鉴别测试

编号	**2.1**	**测试点**	**用户注册过程**	**测试情况**
测试内容及要求	1.通过测试确认用户主体只能被注册 1 次。 2.通过测试确认系统存在能够有效认证用户主体的功能设计。如实名注册中，至少通过查询姓名与身份证号码的匹配度来验证用户主体的真实性。 3.通过测试确认不存在可以直接控制注册用户权限的参数。 4.通过测试确认注册过程包含有效的人机识别，无法通过自动化批量完成。			■已测试 □不具备测试条件 □不适用
编号	**2.2**	**测试点**	**账户权限变化**	**测试情况**
测试内容及要求	1.结合角色权限矩阵，梳理所有涉及权限变化的功能，并确认是否能够最小化满足业务需求。 2.通过测试确认任何角色都不能为自身或其他角色赋予超越自身的权限。 3.通过测试确认任何角色都不能撤销或转移对等权限以及更			■已测试 □不具备测试条件 □不适用

	高权限。			
编号	**2.3**	**测试点**	**账户枚举和弱用户名**	**测试情况**
测试内容及要求	1.通过测试确认登录时无法进行账户枚举，如：提示信息过于明显，未模糊提示。 2.进行账户枚举和弱用户名测试时应尽可能尝试常见用户名与默认用户名。			■已测试 □不具备测试条件 □不适用
编号	**2.4**	**测试点**	**口令信息加密传输**	**测试情况**
测试内容及要求	1.通过测试确认口令信息传输在当前场景下满足 JR/T 0168-2020 的要求。如网银系统在传输口令时应采用双向校验。 2.通过测试确认口令信息传输时至少对口令参数本身使用摘要算法进行加密，或整个请求采用通过国家密码管理部门认可的 HTTPS 协议进行传输。 3.使用 HTTPS 协议的情况下，应通过测试确认口令信息传输不能够通过 HTTP 降级请求。如对于一个必须使用 HTTPS 协议进行访问的应用登录界面，可使用 HTTP 协议访问并成功登录。 4.密码密文每次是否一致，是否加盐。 5.修改密码处，密码是否同注册登录处加密方式一致。			■已测试 □不具备测试条件 □不适用
编号	**2.5**	**测试点**	**默认口令与弱口令**	**测试情况**
测试内容及要求	1.通过访谈及调研的形式确认目标系统不存在统一分发的默认口令，或确认每个账户的默认口令各不相同且无法基于自身分配的口令对其他账户的口令进行预测。 2.通过测试确认不能够使用空口令登录目标系统。 3.通过测试确认不存在能够使用弱口令登录的高权限账户。 4.第三方应用，测试方应通过测试确认第三方应用不存在可预测的默认口令。如出厂口令或可轻易与开发商信息关联的常见口令。			■已测试 □不具备测试条件 □不适用
编号	**2.6**	**测试点**	**账户锁定机制**	**测试情况**
测试内容及要求	1.在生产环境中测试时，应只针对授权使用的测试账号进行账户锁定机制测试。 2.如未设置账户锁定机制，应通过测试确认图片验证码以及其他抗暴力破解措施的有效性。 3.通过测试确认账户锁定机制无法被整体绕过。 4.结合业务需要，确认每次口令锁定时间不低于该业务要求的基准值。			■已测试 □不具备测试条件 □不适用
编号	**2.7**	**测试点**	**认证绕过**	**测试情况**
测试内容及要求	1.通过测试确认内部功能均进行了有效的认证保护，无法通过直接请求非授权访问内部功能。			■已测试 □不具备

	2.通过测试确认不存在能够通过参数直接激活登录认证的功能。如参数 login=on 后能够以某一个固定或指定的权限正常使用相应功能。 3.通过测试确认会话标识或用来标示身份的其他参数不能进行线性预测。 4.通过测试确认无法通过修改响应包的方式简化前端页面分析并获取更多应用入口信息。			测试条件 □不适用
编号	**2.8**	**测试点**	**记住密码功能**	**测试情况**
测试内容及要求	通过测试确认浏览器本地（包括但不限于 Cookie、Local Storage、Session Storage）中没有存储明文密码或哈希。			■已测试 □不具备测试条件 □不适用
编号	**2.9**	**测试点**	**密码策略**	**测试情况**
测试内容及要求	1.通过测试确认目标系统的密码策略满足对应安全级别的要求。如密码长度要求、密码组成要求、密码强制修改周期要求和历史密码策略要求等。 2.通过测试确认目标系统无法通过连续多次更改密码的方式绕过历史密码策略。 3.新旧密码是否可以相同。			■已测试 □不具备测试条件 □不适用
编号	**2.10**	**测试点**	**密码修改及重置**	**测试情况**
测试内容及要求	1.通过测试确认密码修改功能验证了原密码，并确保验证的有效性。 2.使用了短信及电子邮箱验证码，应通过测试确认密码重置功能的关键步骤中新密码重置与短信及电子邮箱验证码校验同时进行，并确认短信及电子邮箱验证码的设计符合基本要求。 3.使用了电子邮箱找回链接，应通过测试确认找回链接中与身份绑定的标识参数超过 32 位且无法被简单模型预测。 4.使用了电子邮箱找回链接，应通过测试确认电子邮箱找回链接的有效时间不超过 12 小时。 5.使用了重置令牌，应通过测试确认重置令牌来源的唯一性。即不应在系统的其他位置发现可以生成该令牌的接口与功能。 6.跳过验证步骤，直接访问修改密码页面，如结合短信验证码绕过。 7.密码找回凭证可以从客户端、html、cookie、URL 中直接获取。 8.在本地验证服务器的返回信息，确定是否执行重置密码；返回信息是可控内容，或者可以得到的内容。			■已测试 □不具备测试条件 □不适用

(三) 授权测试

编号	3.1	测试点	目录遍历、文件包含	测试情况
测试内容及要求	1.应遍历所有通过用户传入文件名调取文件内容的功能，确保无法基于当前 Web 应用运行权限进行指定操作文件查看及下载的操作。 2.通过测试确认传入参数不支持 PHP 封装协议（伪协议）。如 php://input 和 php://filter 等。 3.通过测试确认传入参数不支持通过“../”以及对应的各类编码或变体进行父目录穿越。			■已测试 □不具备测试条件 □不适用
编号	3.2	测试点	目录浏览	测试情况
测试内容及要求	1.通过测试确认 Web 应用各级目录均未开启目录浏览功能。 2.通过测试确认 Web 应用各级目录不存在通过其他信息间接泄露全部或部分目录名称的问题，如版本控制工具残留文件导致的目录或文件名称泄露。			■已测试 □不具备测试条件 □不适用
编号	3.3	测试点	可预测资源定位	测试情况
测试内容及要求	1.对于不便进行权限限制的静态资源，应通过测试确认其名称具备不可预测性，包括但不限于图片、文档和附件等静态资源。如图片名称包含 32 位以上哈希且不可线性预测。 2.充分尝试请求可能的文件名、后缀及相关变体，确保不存在包含敏感信息的可预测资源。如版本控制文件、备份文件和示例文件等。 3.通过测试确认 Web 服务器及中间件的基础配置文件和管理入口，不会因为配置失误导致未授权访问。			■已测试 □不具备测试条件 □不适用
编号	3.4	测试点	授权绕过	测试情况
测试内容及要求	1.如具备条件，测试方应使用管理员权限遍历管理页面和功能并进行记录，且通过测试确保普通用户以及其他非授权用户不具备这些页面及功能的使用权限。 2.通过测试确认管理功能的权限判断逻辑未仅在前端实现。如在未登录状态下请求某个管理页面，会通过增加 JavaScript 的方式引导用户跳转或关闭窗口，但实际管理功能及数据已经加载并可以正常使用。			■已测试 □不具备测试条件 □不适用
编号	3.5	测试点	权限提升	测试情况
测试内容及要求	通过测试确认不存在通过用户输入参数可以直接控制当前账户整体权限的功能实现或接口。如通过增加参数 admin=1 即可使用管理员功能。			■已测试 □不具备测试条件 □不适用

编号	3.6	测试点	不安全的直接对象引用	测试情况
测试内容及要求	1.通过测试确认所有用户输入的与权限相关的线性参数均不存在平行越权的问题。如 ID=150 为当前用户的内容，ID=151 为当前用户所不具备权限的其他用户的内容。 2.在生产系统中，如涉及写与删除操作的平行越权，应至少在另一个测试账户中进行。如不具备另一个测试账户，则应在仿真环境中进行本项测试。 3.进行不安全的直接对象引用测试时，应严格禁止批量跑取数据的行为。如需要进行危害验证，应获取不超过 5 条数据用以证明危害即可。			■已测试 □不具备测试条件 □不适用

(四) 会话管理测试

编号	4.1	测试点	会话管理绕过	测试情况
测试内容及要求	1.应遍历所有通过用户传入文件名调取文件内容的功能，确保无法基于当前 Web 应用运行权限进行指定操作文件查看及下载的操作，通过测试确认 Cookie 中的会话凭证具备不可预测性。 2.通过测试确认会话标识符从一个可信系统，如服务器上创建，而不是在客户端创建。 3.通过测试确认 Cookie 中的会话凭证不能通过目标系统中的其他功能生成，如存在某个功能实现或接口，在传入用户名后可以得到对应用户的会话凭证。 4.在验证会话凭证的不可预测性时，宜采用通过工具生成大量会话凭证样本并进行碰撞的方式进行。			■已测试 □不具备测试条件 □不适用
编号	**4.2**	**测试点**	**Cookie 属性**	**测试情况**
测试内容及要求	1.应通过测试确认 Cookie 中的会话标识设置了 Secure、HttpOnly 和 SameSite 属性。 2.通过测试确认对 HttpOnly 不支持的浏览器不能使用站点功能。 3.通过测试确认目标系统不存在能够绕过 HttpOnly 机制的漏洞，如特定的中间件漏洞以及利用 CORS 特性导致的 XSS 会话劫持等。			■已测试 □不具备测试条件 □不适用
编号	**4.3**	**测试点**	**会话固定**	**测试情况**
测试内容及要求	1.通过测试确认用户登录成功后目标系统会自动更新会话标识。 2.通过测试确认当用户携带一个通过 URL 传递的指定的会话标识进行用户认证后，该会话标识不会生效。			■已测试 □不具备测试条件 □不适用

编号	4.4	测试点	会话令牌泄露	测试情况
测试内容及要求	通过测试确认所有涉及身份认证的关键参数均不能通过 GET 方式传输。如用户名密码对，会话标识以及其他能够独立通过身份校验的各类凭据。			■已测试 □不具备测试条件 □不适用
编号	**4.5**	**测试点**	**CSRF 跨站请求伪造**	**测试情况**
测试内容及要求	1.梳理并记录所有与身份强相关的单向操作，包括但不限于不需要原密码的密码修改功能、增加用户功能、删除用户功能、赋予用户权限功能、转账功能、发送公告功能等。应通过测试确保上述功能不存在 CSRF 问题。 2.使用 Referer 校验，则应通过测试确认不存在域内的 CSRF 漏洞。 3.使用 Token 校验，则应通过测试确认 Token 验证与会话标识强相关。 4.使用双重校验，则应通过测试确认校验码不可预测及不可绕过。 5.使用图形验证码，则应通过测试确认图形验证码不可预测及不可绕过。 6.通过测试确认目标系统无法进行 JSON 和 JSONP 劫持攻击。			■已测试 □不具备测试条件 □不适用
编号	**4.6**	**测试点**	**登出功能与会话超时**	**测试情况**
测试内容及要求	1.通过测试确认用户界面中存在登出功能，并确认登出功能的有效性。 2.通过测试确认目标系统存在无动作前提下的自动登出时间设置，且不长于 10 分钟。			■已测试 □不具备测试条件 □不适用
编号	**4.7**	**测试点**	**会话变量重载**	**测试情况**
测试内容及要求	通过测试确认目标系统的每次会话变量重载都在充分认证的基础之上进行。如任何未登录的用户在访问某个页面后都被动激活了登录会话，那么在该页面之前应存在用户身份认证的逻辑。			■已测试 □不具备测试条件 □不适用

(五) 输入验证测试

编号	5.1	测试点	XSS 跨站脚本攻击	测试情况
测试内容及要求	1.测试确认输入过滤及输出编码措施的有效性。使用的测试手段包括但不限于以下方式：结合上下文环境引入自定义的 HTML、XML、JavaScript、CSS 代码，通过等价替换、变异等方式绕过黑白名单检测，利用上传功能直接上传含有跨站脚本的静态页面等。			■已测试 □不具备测试条件 □不适用

	2.在仿真环境中，通过测试确认当前目标系统中输入的跨站脚本不会作用于其他系统。如 XSS 盲打。 3.通过测试确认目标系统不存在可以指定伪协议、JavaScript、Data-ur 和 Blob 等而导致的 XSS 漏洞。 4.梳理并记录所有能够将用户输入内容存入数据库并回显至页面的功能。包括但不限于用户名、头像、用户信息、转账信息、订单、对账单、论坛、留言板、站内搜索和查询等功能。 5.如使用了 CSP 技术，应通过测试确认当前 CSP 配置无法被绕过。 6.通过测试确保目标应用服务在 Internet Explorer、Chrome、Firefox 和 Safari 等浏览器的主流版本均不存在可利用的跨站脚本漏洞。			
编号	**5.2**	**测试点**	**SSRF**	**测试情况**
测试内容及要求	1.应在所有可能调用内部或外部第三方系统的位置进行充分的 SSRF 测试尝试。包括但不限于直接通过参数传递 IP 地址的功能、传递端口号的功能、传递第三方 URL 的功能以及传递第三方回显数据的功能等。 2.通过测试确认传入的 URL 参数仅支持 HTTP(S)协议，不应响应 file://、gopher://、ftp://和 dict://等其他网络协议。			■已测试 □不具备测试条件 □不适用
编号	**5.3**	**测试点**	**HTTP 谓词篡改**	**测试情况**
测试内容及要求	1.通过测试确认目标系统是否开启了 Webdav。 2.在开启了 Webdav 的前提下，应通过测试确认目标系统无法通过 Webdav 缺陷配置上传 Webshell。			■已测试 □不具备测试条件 □不适用
编号	**5.4**	**测试点**	**HTTP 参数污染**	**测试情况**
测试内容及要求	1.通过测试确认在引入多个同名参数时，安全限制与参数执行始终保持一致。 2.通过测试确认在引入多个同名参数时，目标系统在接受了多个参数值组合的前提下无法绕过安全限制。			■已测试 □不具备测试条件 □不适用
编号	**5.5**	**测试点**	**SQL 注入**	**测试情况**
测试内容及要求	涉及增、删、改的注入测试，应在仿真环境下进行。严禁在生产环境中进行增、删、改相关的各类 SQL 注入测试。包括但不限于通过堆叠注入引入完整的增删改语句等。			■已测试 □不具备测试条件 □不适用
编号	**5.6**	**测试点**	**XML 注入**	**测试情况**
测试内容及要求	1.通过尝试插入 XML 元字符以及节点的方式充分测试当前功能中是否存在 XML 解析的可能。 2.目标系统使用了 XML 数据库的前提下，应通过测试确认对应功能不存在 XML 标签注入问题。			■已测试 □不具备测试条件 □不适用

	3.应通过测试确认目标系统不存在 XML 外部实体注入问题。			
编号	**5.7**	**测试点**	**其他注入**	**测试情况**
测试内容及要求	1.目标系统使用了 LDAP 服务器的前提下，应通过测试确认对应功能不存在 LDAP 注入问题。 2.通过测试确认目标系统不存在系统命令注入问题。 3.通过测试确认目标系统是否开启了 SSI 支持，若开启应确认不存在 SSI 注入问题。 4.在目标系统使用了 XPath 查询方式的前提下，应通过测试确认对应功能不存在 XPath 注入问题。可以尝试使用与 SQL 注入通用的测试记录覆盖部分 XPath 注入测试。 5. 在测试 Web 电子邮箱系统以及具备 Web 电子邮箱功能的其他应用系统时，应通过测试确认目标系统不存在 IMAP/SMTP 注入问题。 6.通过测试确认目标系统不存在 HTTPHeader 参数注入，如 X-Forwarded-For 注入问题。 7.通过测试确认目标系统不存在由于 CRLF 注入所导致的 HTTP 响应分割问题。 8.通过模糊测试与域名解析记录相结合的方式，确认目标系统不存在命令注入问题。 9.通过测试确认目标系统不存在代码注入问题，包括但不限于应用代码注入、模板注入或表示层语言注入问题。 10.通过灰盒或白盒测试的方式，确认目标系统不存在各类注入问题。			■已测试 □ 不具备测试条件 □不适用
编号	**5.8**	**测试点**	**孵化漏洞**	**测试情况**
测试内容及要求	在一些复杂的业务逻辑场景下，应通过测试确认目标系统不存在多个条件组合达成时才能成功利用的逻辑漏洞。			■已测试 □ 不具备测试条件 □不适用
编号	**5.9**	**测试点**	**HTTP 分割/伪造**	**测试情况**
测试内容及要求	在使用了安全限制的场景下，应通过测试确认安全限制不会通过 HTTP 分割/伪造的方式绕过。			■已测试 □ 不具备测试条件 □不适用

(六) 错误处理测试

编号	**6.1**	**测试点**	**错误处理**	**测试情况**

测试内容及要求	1.维护一个易于触发服务端错误的模糊测试列表，并在非增删改功能中进行模糊测试以获取充足的错误响应样本。 2.充分评估错误响应中暴露的技术细节，并通过这些细节充分测试可能导致风险的各类威胁。 3.通过报错信息，错误响应，是否会泄露服务器版本信息、中间件信息、数据库信息等等。	■已测试 □不具备测试条件 □不适用

(七) 密码学测试

编号	7.1	测试点	传输层防护及敏感数据	测试情况
测试内容及要求	1.采用专有的线上及线下工具测试 SSL/TLS 的整体安全性。线上及线下工具的选择和使用应遵循金融机构的相关管理制度。 2.通过测试确认目标系统的 SSL/TLS 版本及配置不存在已知的高危漏洞。 3.目标系统不采用有效的 HTTPS 配置时，应通过测试确认目标系统无明文传输用户凭据问题。 4.目标系统及客户端之间使用双向校验时，应通过测试确认无法实施有效的中间人攻击。			■已测试 □不具备测试条件 □不适用

(八) WEB 客户端测试

编号	8.1	测试点	客户端 URL 重定向	测试情况
测试内容及要求	通过测试确认目标系统不存在可以指定目标域名进行直接或二次跳转的功能。如用户在访问构造页面后，需经过登录再进行跳转的场景属于二次跳转。			■已测试 □不具备测试条件 □不适用
编号	**8.2**	**测试点**	**跨域资源共享**	**测试情况**
测试内容及要求	通过测试确认目标系统是否开启了 CORS 功能。在开启了 CORS 功能的前提下，应通过测试确认域限制使用白名单机制。			■已测试 □不具备测试条件 □不适用
编号	**8.3**	**测试点**	**Flash 跨站**	**测试情况**
测试内容及要求	通过对 Flash 文件进行反编译，测试是否存在能够导致 XSS 的未初始化全局变量以及不安全方法。			■已测试 □不具备测试条件 □不适用

(九) 敏感信息泄露测试

编号	9.1	测试点	敏感信息泄露	测试情况
测试内容及要求	1.弱文件，对系统请求和回复过程中的报文进行分析，验证是否存在敏感信息泄露风险。 2.源代码，对系统请求和回复过程中的报文进行分析，验证是否存在敏感信息泄露风险。 3.配置文件、JDBC，对系统请求和回复过程中的报文进行分析，验证是否存在敏感信息泄露风险。 4.数据库文件，对系统请求和回复过程中的报文进行分析，验证是否存在敏感信息泄露风险。			■已测试 □不具备测试条件 □不适用

(十) 中间件测试

编号	10.1	测试点	中间件	测试情况
测试内容及要求	1.对系统部署使用的中间件可能存在的安全风险进行测试，如 tomcat 后台弱口令、weblogic 弱口令、weblogic 反序列化漏洞，以及对中间件中默认配置引起的信息泄露风险进行漏洞扫描。 2.WebServer、JBOSS、WebSphere 等中间件远程代码执行。 3.Struts2、Spring、shiro 等代码执行。 4.Struts2 命令执行漏洞等各种系统使用的开源框架漏洞进行测试。			■已测试 □不具备测试条件 □不适用

(十一) 配置错误及框架漏洞测试

编号	11.1	测试点	安全配置错误	测试情况
测试内容及要求	1.高危端口 22、139、445、3389、7001。 2.数据库 xp_cmdshell、口令。 3.jQuery 低版本漏洞等各种系统使用的开源框架漏洞进行测试。			■已测试 □不具备测试条件 □不适用

(十二) App 客户端测试

编号	12.1	测试点	客户端（APK、Android）安全	测试情况
测试内容及要求	1.App 客户端是否可被编译。 2.客户端是否可被二次打包。			■已测试 □不具备

	3.客户端是否可被调试。 4.安全输入（替换输入框原文、逐字符加密、键盘窃听、采用自定义软键盘、运行环境）。 5.运行环境检测，是否在 root、模拟器、越狱环境下打开。 6.组件安全。 7.APK 是否签名。 8.是否及时清除敏感信息缓存。 9.防截屏、防录屏措施。 10.权限控制（如：日志可被打印、获取用户权限过多等）。 11.敏感信息展示。	测试条件 □不适用

五、 漏洞发现详情

(一)“盒条件”关联厂级管理子系统（V2.0）1

1. 高危问题

无。

2. 中危问题

无。

3. 低危问题

无。

(二)“条零”关联物流中心级管理子系统（V2.0）2

1. 高危问题

无。

2. 中危问题

无。

3. 低危问题

无。

(三)“条零”关联现场管理子系统（V2.0）3

1. 高危问题

无。

2. 中危问题

无。

3. 低危问题

无。

(四)“盒条”关联人工作业单元（V2.0）4

1. 高危问题

无。

2. 中危问题

无。

3. 低危问题

无。

(五)“盒条”关联现场管理子系统（V2.0）5

1. 高危问题

无。

2. 中危问题

无。

3. 低危问题

无。

(六)“条件”关联人工作业单元（V2.0）6

1. 高危问题

无。

2. 中危问题

无。

3. 低危问题

无。

(七)“条件”关联现场管理子系统（V2.0）7

1. 高危问题

无。

2. 中危问题

无。

3. 低危问题

无。

(八)“盒条件”关联人工作业单元 apk 8

1. 高危问题

(1) Webview File 同源策略绕过漏洞

漏洞路径	app-release-htj-1103.apk

<table>
<tr><td>漏洞类型</td><td>□业务逻辑漏洞 □身份鉴别 □授权测试 □会话管理 □输入验证 □错误处理 □密码学 □WEB 客户端 ■敏感信息泄露 □中间件 □配置错误及框架漏洞 □App 客户端 □其他</td></tr>
<tr><td>漏洞描述</td><td>JavaScript 的延时执行能够绕过 file 协议的同源检查，并能够访问受害应用的所有私有文件，即通过 WebView 对 Javascript 的延时执行和将当前 Html 文件删除掉并软连接指向其他文件就可以读取到被符号链接所指的文件，然后通过 JavaScript 再次读取 HTML 文件，即可获取到被符号链接所指的文件。大多数使用 WebView 的应用都会受到该漏洞的影响，恶意应用通过该漏洞，可在无特殊权限下盗取应用的任意私有文件，尤其是浏览器，可通过利用该漏洞，获取到浏览器所保存的密码、Cookie、收藏夹以及历史记录等敏感信息，从而造成敏感信息泄露。</td></tr>
<tr><td>漏洞证明</td><td>apk 漏洞扫描
<table><tr><td>测评详细信息</td><td>1.
[文件]:
com/tobacco/qrcode/component/WebViewManage/WebViewConstructor
[方法]:
private initWebView()V</td></tr></table></td></tr>
<tr><td>修复建议</td><td>➢ 将不必要导出的组件设置为不导出，并显式设置所注册组件的“android:exported”属性为 false；
➢ 如果需要导出组件，禁止使用 File 域：WebView.getSettings.setAllowFileAccess(false);
➢ 如果需要使用 File 协议，禁止 File 协议调用 JavaScript：WebView.getSettings.setJavaScriptEnabled(false)。</td></tr>
<tr><td>复测情况</td><td>经验证，该风险问题已修复，修复记录如下：
<table><tr><td>测评结果</td><td>安全</td></tr><tr><td>测评结果描述</td><td>该 Apk 程序不存在 webview File 同源策略绕过的漏洞。</td></tr></table></td></tr>
</table>

2.中危问题

(1) Webview 绕过证书校验漏洞

<table>
<tr><td>漏洞路径</td><td>app-release-htj-1103.apk</td></tr>
<tr><td>漏洞类型</td><td>□业务逻辑漏洞 ■身份鉴别 □授权测试 □会话管理 □输入验证 □错误处理 □密码学 □WEB 客户端 □敏感信息泄露 □中间件 □配置错误及框架漏洞 □App 客户端 □其他</td></tr>
<tr><td>漏洞描述</td><td>客户端的 Webview 组件访问使用 HTTPS 协议加密的 url 时，如果服务器证书校验错误，客户端应该拒绝继续加载页面。但如果重载 WebView 的 onReceivedSslError()函数并在其中执行 handler.proceed()，客户端可以绕过证书校验错误继续访问此非法 URL。这样将会导致“中间人攻击”，攻击者</td></tr>
</table>

	冒充服务器与手机客户端进行交互，同时冒充手机客户端与服务器进行交互，在充当中间人转发信息的时候，窃取手机号，账号，密码等敏感信息。
漏洞证明	apk 漏洞扫描 测评详细信息：[文件]：com/tobacco/qrcode/component/WebViewManage/WebViewConstructor [方法]：onReceivedSslError(Landroid/webkit/WebView;Landroid/webkit/SslErrorHandler;Landroid/net/http/SslError;)V
修复建议	➢ 在 Webveiw 组件中不要调用 onReceivedSslError()函数的 handler.proceed()方法忽略证书错误，建议采用默认的处理方法 handler.cancle()，停止加载证书错误页面。
复测情况	经验证，该风险问题已修复，修复记录如下： 测评结果：安全 测评结果描述：该 App 应用不存在 webview 组件绕过证书校验的漏洞。

(2) 不安全的浏览器调用漏洞

漏洞路径	app-release-htj-1103.apk
漏洞类型	□业务逻辑漏洞 □身份鉴别 ■授权测试 □会话管理 □输入验证 □错误处理 □密码学 □WEB 客户端 □敏感信息泄露 □中间件 □配置错误及框架漏洞 □App 客户端 □其他
漏洞描述	Chrome V8 引擎 3.20 至 4.2 版本中存在远程代码执行漏洞（CNNVD-201608-414）。该漏洞是由于源代码中“observe_accept_invalid”异常类型被误写为“observe_invalid_accept”，造成 kMessages 关键对象信息泄露，从而可利用该漏洞执行任意代码。远程攻击者可通过诱使用户扫描二维码或者诱使用户点击恶意链接对应用进行攻击，可能导致用户隐私泄露，如通讯录，短信，录音，录像等；用户财产损失，如窃取支付密码、钱包密码等；远程控制手机等。
漏洞证明	apk 漏洞扫描 com/tobacco/qrcode/component/WebViewManage/WebViewConstructor [方法]： private initWebView()V
修复建议	➢ 开发者需要在应用调用外部浏览器时对引擎版本进行检测，当发现调用 Chrome V8 引擎并且版本低于 4.2 时停止调用外部浏览器并且提示用户对调用的系统浏览器进行升级或者修改系统默认的浏览器； ➢ 集成第三方 sdk 实现浏览器功能，如腾讯的 x5sdk(最新版)。

复测情况	经验证，该风险问题已修复，修复记录如下： 测评结果：安全 测评结果描述：该 App 中不存在不安全的浏览器调用漏洞。

3.低危问题

(1) InnerHTML 的 XSS 攻击漏洞

漏洞路径	app-release-htj-1103.apk
漏洞类型	□业务逻辑漏洞 □身份鉴别 □授权测试 □会话管理 ■输入验证 □错误处理 □密码学 □WEB 客户端 □敏感信息泄露 □中间件 □配置错误及框架漏洞 □App 客户端 □其他
漏洞描述	DOM 型 XSS 漏洞是基于文档对象模型（Document Object Model）的一种漏洞。它的攻击代码不需要服务器解析响应，而是通过浏览器端的 DOM 解析触发 XSS。客户端上的 JavaScript 脚本可以访问浏览器的 DOM 并修改页面的内容，不依赖服务器的数据，直接从浏览器端获取数据并执行。 在 JavaScript 中给 DOM 的 innerHTML 属性赋值一个<script>标签，是一个非常普遍的 xss 注入点。如果攻击者利用该漏洞进行攻击，可能会导致账号或 Cookie 信息被窃取，从而冒充管理者登录后台进行数据篡改等恶意操作。
漏洞证明	apk 漏洞扫描 测评详细信息： 1. [文件]： /assets/web/assets/htjscrap-legacy.de444a20.js [代码]： ument.createElement("style");e.innerHTML="*[data-v-770acd78]{margin:0;padding:0} 2. [文件]： /assets/web/assets/qrCodeInfohtj-legacy.4a1c846e.js
修复建议	➢ 使用 textContent； ➢ 使用第三方过滤了危险字符的框架，来给 DOM 复制。例如 jquery 的 html()函数。
复测情况	经验证，该风险问题未修复。 漏洞未修复，被测方接受风险，暂不进行整改。

(2) 残留账户密码信息检测

漏洞路径	app-release-htj-1103.apk

<table>
<tr><td>漏洞类型</td><td>□业务逻辑漏洞 □身份鉴别 ■授权测试 □会话管理 □输入验证 □错误处理 □密码学 □WEB 客户端 □敏感信息泄露 □中间件 □配置错误及框架漏洞 □App 客户端 □其他</td></tr>
<tr><td>漏洞描述</td><td>移动应用发布包中如果存在残留的账户、密码信息，可能会被盗取并恶意利用在正式服务器上进行攻击，例如账号重试，攻击安全薄弱的测试服务器以获取服务器安全漏洞或者逻辑漏洞。</td></tr>
<tr><td>漏洞证明</td><td>apk 漏洞扫描
<table><tr><td>测评详细信息</td><td>[文件]：
androidx/core/util/PatternsCompat
[代码]：
.field private static final USER_INFO:Ljava/lang/String; = (?:[a-zA-Z0-9$-_.+!*(),;?&=]|(?:%[a-fA-F0-9]{2})){1,64}(?::(?:[a-zA-Z0-9$-_.+!*(),;?&=]|(?:%[a-fA-F0-9]{2})){1,25})?@</td></tr></table></td></tr>
<tr><td>修复建议</td><td>➢ 核查所有残留的账户和密码信息，删除与业务无关的账户和密码；
➢ 尽量不要将与客户端业务相关的账户密码信息以硬编码的方式写在应用客户端中。</td></tr>
<tr><td>复测情况</td><td>经验证，该风险问题已修复，修复记录如下：<table><tr><td>测评结果</td><td>安全</td></tr><tr><td>测评结果描述</td><td>该 App 应用中未包含残留的账户、密码信息。</td></tr></table></td></tr>
</table>

(3) zip 文件解压目录遍历漏洞

<table>
<tr><td>漏洞路径</td><td>app-release-htj-1103.apk</td></tr>
<tr><td>漏洞类型</td><td>□业务逻辑漏洞 □身份鉴别 ■授权测试 □会话管理 □输入验证 □错误处理 □密码学 □WEB 客户端 □敏感信息泄露 □中间件 □配置错误及框架漏洞 □App 客户端 □其他</td></tr>
<tr><td>漏洞描述</td><td>该 App 中存在解压 zip 文件时可导致目录遍历的漏洞。</td></tr>
<tr><td>漏洞证明</td><td>apk 漏洞扫描
<table><tr><td>测评详细信息</td><td>1.
[文件]：
kim/hsl/multipledex/ZipUtils
[方法]：
public static unZipApk(Ljava/io/File;Ljava/io/File;)V</td></tr></table></td></tr>
<tr><td>修复建议</td><td>➢ 当 App 程序中使用 zipInputStream 类对 Zip 压缩包进行解压操作时，在 ZipEntry.getName()获取的文件名后，必须添加过滤代码对文件名中可能包含的”../” 进行过滤判断，以提示用户并终止可能发生的异常操作。以下为修复代码示例：
while((ZipEntry =zipInputStream.getNextEntry())!=null</td></tr>
</table>

	{String entryName=zipEntry.getnName();
	if (entryName.contains("../"))
	{
	throw new Exception("发现不安全的 zip 文件解压路径！ ")
	}
	}

复测情况	经验证，该风险问题未修复。 漏洞未修复，被测方接受风险，暂不进行整改。

(九)“条零”关联人工作业单元 apk 9

1. 高危问题

(1) Webview File 同源策略绕过漏洞

漏洞路径	app-release-tj-1103.apk
漏洞类型	□业务逻辑漏洞 □身份鉴别 □授权测试 □会话管理 □输入验证 □错误处理 □密码学 □WEB 客户端 ■敏感信息泄露 □中间件 □配置错误及框架漏洞 □App 客户端 □其他
漏洞描述	JavaScript 的延时执行能够绕过 file 协议的同源检查，并能够访问受害应用的所有私有文件，即通过 WebView 对 Javascript 的延时执行和将当前 Html 文件删除掉并软连接指向其他文件就可以读取到被符号链接所指的文件，然后通过 JavaScript 再次读取 HTML 文件，即可获取到被符号链接所指的文件。大多数使用 WebView 的应用都会受到该漏洞的影响，恶意应用通过该漏洞，可在无特殊权限下盗取应用的任意私有文件，尤其是浏览器，可通过利用该漏洞，获取到浏览器所保存的密码、Cookie、收藏夹以及历史记录等敏感信息，从而造成敏感信息泄露。
漏洞证明	apk 漏洞扫描 测评详细信息： 1. [文件]: com/tobacco/qrcode/component/WebViewManage/WebViewConstructor [方法]: private initWebView()V
修复建议	➢ 将不必要导出的组件设置为不导出，并显式设置所注册组件的“android:exported”属性为 false； ➢ 如果需要导出组件，禁止使用 File 域：WebView.getSettings.setAllowFileAccess(false);

	➢ 如果需要使用 File 协议，禁止 File 协议调用 JavaScript：WebView.getSettings.setJavaScriptEnabled(false)。
复测情况	经验证，该风险问题已修复，修复记录如下： 测评结果：安全 测评结果描述：该 Apk 程序不存在 webview File 同源策略绕过的漏洞。

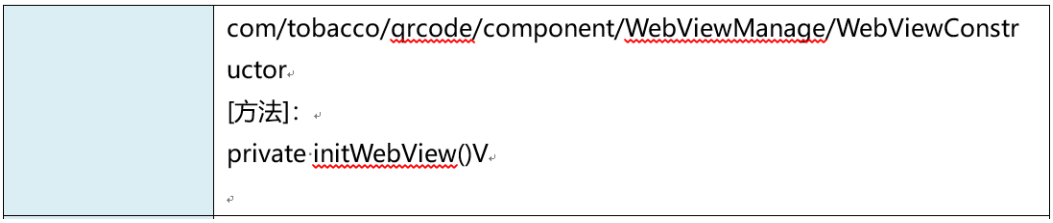
2. 中危问题

(1) Webview 绕过证书校验漏洞

漏洞路径	app-release-tj-1103.apk
漏洞类型	□业务逻辑漏洞 ■身份鉴别 □授权测试 □会话管理 □输入验证 □错误处理 □密码学 □WEB 客户端 □敏感信息泄露 □中间件 □配置错误及框架漏洞 □App 客户端 □其他
漏洞描述	客户端的 Webview 组件访问使用 HTTPS 协议加密的 url 时，如果服务器证书校验错误，客户端应该拒绝继续加载页面。但如果重载 WebView 的 onReceivedSslError()函数并在其中执行 handler.proceed()，客户端可以绕过证书校验错误继续访问此非法 URL。这样将会导致“中间人攻击”，攻击者冒充服务器与手机客户端进行交互，同时冒充手机客户端与服务器进行交互，在充当中间人转发信息的时候，窃取手机号，账号，密码等敏感信息。
漏洞证明	apk 漏洞扫描 测评详细信息：[文件]: com/tobacco/qrcode/component/WebViewManage/WebViewConstructor [方法]: onReceivedSslError(Landroid/webkit/WebView;Landroid/webkit/SslErrorHandler;Landroid/net/http/SslError;)V
修复建议	➢ 在 Webveiw 组件中不要调用 onReceivedSslError()函数的 handler.proceed()方法忽略证书错误，建议采用默认的处理方法 handler.cancle()，停止加载证书错误页面。
复测情况	经验证，该风险问题已修复，修复记录如下： 测评结果：安全 测评结果描述：该 App 应用不存在 webview 组件绕过证书校验的漏洞。

(2) 不安全的浏览器调用漏洞

漏洞路径	app-release-tj-1103.apk
漏洞	□业务逻辑漏洞 □身份鉴别 ■授权测试 □会话管理 □输入验证 □错误处理 □密码学 □WEB 客户端 □敏感信息泄露 □中间件

类型	□配置错误及框架漏洞 □App 客户端 □其他
漏洞描述	Chrome V8 引擎 3.20 至 4.2 版本中存在远程代码执行漏洞（CNNVD-201608-414）。该漏洞是由于源代码中“observe_accept_invalid”异常类型被误写为“observe_invalid_accept”，造成 kMessages 关键对象信息泄露，从而可利用该漏洞执行任意代码。远程攻击者可通过诱使用户扫描二维码或者诱使用户点击恶意链接对应用进行攻击，可能导致用户隐私泄露，如通讯录，短信，录音，录像等；用户财产损失，如窃取支付密码、钱包密码等；远程控制手机等。
漏洞证明	apk 漏洞扫描 
修复建议	➢ 开发者需要在应用调用外部浏览器时对引擎版本进行检测，当发现调用 Chrome V8 引擎并且版本低于 4.2 时停止调用外部浏览器并且提示用户对调用的系统浏览器进行升级或者修改系统默认的浏览器; ➢ 集成第三方 sdk 实现浏览器功能，如腾讯的 x5sdk(最新版)。
复测情况	经验证，该风险问题已修复，修复记录如下： 测评结果：安全 测评结果描述：该 App 中不存在不安全的浏览器调用漏洞。

3. 低危问题

(1) InnerHTML 的 XSS 攻击漏洞

漏洞路径	app-release-htj-1103.apk
漏洞类型	□业务逻辑漏洞 □身份鉴别 □授权测试 □会话管理 ■输入验证 □错误处理 □密码学 □WEB 客户端 □敏感信息泄露 □中间件 □配置错误及框架漏洞 □App 客户端 □其他
漏洞描述	DOM 型 XSS 漏洞是基于文档对象模型（Document Object Model）的一种漏洞。它的攻击代码不需要服务器解析响应，而是通过浏览器端的 DOM 解析触发 XSS。客户端上的 JavaScript 脚本可以访问浏览器的 DOM 并修改页面的内容，不依赖服务器的数据，直接从浏览器端获取数据并执行。 在 JavaScript 中给 DOM 的 innerHTML 属性赋值一个<script>标签，是一个非常普遍的 xss 注入点。如果攻击者利用该漏洞进行攻击，可能会导致账号或 Cookie 信息被窃取，从而冒充管理者登录后台进行数据篡改等恶意操作。
漏洞	apk 漏洞扫描

证明	测评详细信息：1. [文件]： /assets/web/assets/htjscrap-legacy.de444a20.js [代码]： ument.createElement("style");e.innerHTML="*[data-v-770acd78]{margin:0;padding:0} 2. [文件]： /assets/web/assets/qrCodeInfohtj-legacy.4a1c846e.js
修复建议	➢ 使用 textContent； ➢ 使用第三方过滤了危险字符的框架，来给 DOM 复制。例如 jquery 的 html()函数。
复测情况	经验证，该风险问题未修复。 漏洞未修复，被测方接受风险，暂不进行整改。

(2) 残留账户密码信息检测

漏洞路径	app-release-tj-1103.apk
漏洞类型	□业务逻辑漏洞 □身份鉴别 ■授权测试 □会话管理 □输入验证 □错误处理 □密码学 □WEB 客户端 □敏感信息泄露 □中间件 □配置错误及框架漏洞 □App 客户端 □其他
漏洞描述	移动应用发布包中如果存在残留的账户、密码信息，可能会被盗取并恶意利用在正式服务器上进行攻击，例如账号重试，攻击安全薄弱的测试服务器以获取服务器安全漏洞或者逻辑漏洞。
漏洞证明	apk 漏洞扫描 测评详细信息：[文件]： androidx/core/util/PatternsCompat [代码]： .field private static final USER_INFO:Ljava/lang/String; = (?:[a-zA-Z0-9$-_.+!*(),;?&=]|(?:%[a-fA-F0-9]{2})){1,64}(?::(?:[a-zA-Z0-9$-_.+!*(),;?&=]|(?:%[a-fA-F0-9]{2})){1,25})?@
修复建议	➢ 核查所有残留的账户和密码信息，删除与业务无关的账户和密码； ➢ 尽量不要将与客户端业务相关的账户密码信息以硬编码的方式写在应用客户端中。
复测情况	经验证，该风险问题已修复，修复记录如下： 测评结果：安全 测评结果描述：该 App 应用中未包含残留的账户、密码信息。

(3) zip 文件解压目录遍历漏洞

<table>
<tr><td>漏洞路径</td><td>app-release-htj-1103.apk</td></tr>
<tr><td>漏洞类型</td><td>□业务逻辑漏洞 □身份鉴别 ■授权测试 □会话管理 □输入验证 □错误处理 □密码学 □WEB 客户端 □敏感信息泄露 □中间件 □配置错误及框架漏洞 □App 客户端 □其他</td></tr>
<tr><td>漏洞描述</td><td>该 App 中存在解压 zip 文件时可导致目录遍历的漏洞。</td></tr>
<tr><td>漏洞证明</td><td>apk 漏洞扫描
<table><tr><td>测评详细信息</td><td>1.
[文件]:
kim/hsl/multipledex/ZipUtils
[方法]:
public static unZipApk(Ljava/io/File;Ljava/io/File;)V</td></tr></table></td></tr>
<tr><td>修复建议</td><td>➢ 当 App 程序中使用 zipInputStream 类对 Zip 压缩包进行解压操作时，在 ZipEntry.getName()获取的文件名后，必须添加过滤代码对文件名中可能包含的”../” 进行过滤判断，以提示用户并终止可能发生的异常操作。以下为修复代码示例：
while((ZipEntry =zipInputStream.getNextEntry())!=null
{String entryName=zipEntry.getnName();
if (entryName.contains("../"))
{
throw new Exception("发现不安全的 zip 文件解压路径！ ")
}
}</td></tr>
<tr><td>复测情况</td><td>经验证，该风险问题未修复。
漏洞未修复，被测方接受风险，暂不进行整改。</td></tr>
</table>

六、 漏洞扫描结论与建议

(一) 安全等级评定

经过本次漏洞扫描，我们对此系统的安全评价是:相对安全系统（“盒条件”关联厂级管理子系统（V2.0）1、“条零”关联物流中心级管理子系统（V2.0）2、“条零”关联现场管理子系统（V2.0）

3、“盒条”关联人工作业单元（V2.0）4、“盒条”关联现场管理子系统（V2.0）5、“条件”关联人工作业单元（V2.0）6、“条件”关联现场管理子系统（V2.0）7）、不安全系统（“盒条件”关联人工作业单元 apk 8、“条零”关联人工作业单元 apk 9）。

安全等级	资源内容描述
不安全系统 （符合任何一个条件）	1. 存在一个或一个以上高危的系统安全问题，可直接导致系统受到破坏； 2. 与其他非安全系统连接，同时存在相互信任关系（或账号互通）的主机； 3. 发现已经被人入侵且留下后门的主机； 4. 存在 3 个以上中危安全问题； 5. 与其他非安全系统在一个共享网络中，同时维护明文传输口令； 6. 完全不能抵抗小规模的拒绝服务攻击。
一般安全系统 （符合任何一个条件）	1. 存在一个或一个以上中危安全问题； 2. 开放过多服务，同时可能被利用来进行拒绝服务的主机； 3. 与其他非安全系统直接连接，但暂时不存在直接信任(或账号互通)关系； 4. 维护通过明文的方式传递信息； 5. 存在三个以上低危安全问题； 6. 只能抵御最低级的拒绝服务攻击。
相对安全系统 （符合全部条件）	1. 最多存在 1-2 个低危安全问题； 2. 维护方式安全； 3. 与不安全或一般安全系统相对独立； 4. 能抵挡一定规模的拒绝服务攻击。

(二) 已有的安全措施分析

从对服务器系统的探测得出只开放了特定应用的端口，这可能是因为利用防火墙等防护设备做了一定程度的安全策略，很大程度上提高了安全性。

通过安全漏洞扫描，没有发现任何应用层和系统层的安全漏洞，管理人员应该为系统更新了关键补丁，避免了系统存在大量补丁级漏洞的风险。从这一点上来看补丁及时更新的工作是非常有意义的，能够一定程度的降低风险。

(三) 安全建议

经过本次漏洞扫描，我们发现被检测系统中存在的安全问题均已被修复，我们建议采用如下方式持续提升信息系统安全管理和防护水平，为业务的平稳运行和快速发展保驾护航。

1. 及时安装最新的安全补丁

及时安装最新的安全补丁。这有助于解决已知的一些安全漏洞，提高系统的安全性，使得攻击者即使绕过防火墙进入了系统也无法轻易入侵内部主机。

2. 进行系统级的安全加固配置

对操作系统和应用系统本身进行安全加固可以大大提高系统的抗攻击的能力。例如，设置合理的口令策略、进行文件系统的访问控制、以及网络访问控制等。

3. Web 安全编程

即使有客户端验证，也不要相信客户端的输入！

- 请求 URL 的参数部分
- HTML 表单通过 POST 或 GET 请求提交的数据
- 在客户端临时保存的数据（也就是 Cookie）
- 数据库查询

4. 定期进行安全审计

虽然我们在本次检测中发现了部分安全隐患，并且这些隐患已得到解决或能够在短时间内解决。我们仍然建议您定期进行类似的安全测试，保障不断发展的动态网络的持续安全。

5. 安全复检

在修复此次发现的安全漏洞并完成系统及应用的安全加固后，建议再次进行安全检测，以校验评估安全状态，并确保无其他安全问题存在。

（以下空白）

优质高效的服务　　准确有效的数据

全面公正的测试　　科学合理的结论

国家金融IC卡安全检测中心
National Financial IC Card Security Test Center
银行卡检测中心
Bank Card Test Center

欢迎广大客户使用在线委托、电话、传真、电子邮件和现场洽谈等方式办理业务，中心将为客户提供优质高效、方便快捷的专业技术服务。

在线委托：中心网站（www.bctest.com）在线委托平台

电　　话：86-10-81131728；**传　　真：**86-10-81131500

官方微博：　　**官方微信：**

地　　址：中国北京市石景山区实兴大街 30 号院 18 号楼

邮　　编：100041