ICS 03.060
A11

JR

中华人民共和国金融行业标准

JR/T 0191—2020

证券期货业软件测试指南 软件安全测试

Guide for securities and futures industry software test—Software security testing

2020-07-10 发布　　2020-07-10 实施

中国证券监督管理委员会　发布

目　　次

前　言

本标准按照GB/T1.1—2009给出的规则起草。

本标准由全国金融标准化技术委员会证券分技术委员会（SAC/TC180/SC4）提出。

本标准由全国金融标准化技术委员会(SAT/TC180)归口。

本标准起草单位：中国证券监督管理委员会信息中心、大连商品交易所、证券期货业信息技术测试中心（大连）、中证信息技术服务有限责任公司、上海证券交易所、深圳证券交易所、上海期货交易所、中国金融期货交易所、国泰君安证券股份有限公司、恒生电子股份有限公司、北京梆梆安全科技有限公司。

本标准主要起草人：姚前、刘铁斌、周云晖、许强、李向东、俞枫、刘军、孙瑞超、刘进、丁新杰、董琳、肖昱、高心远、高锋远、李婷婷、沙明、谢冉、林林、陈冬严、杨硕、刘舒骐。

证券期货业软件测试指南 软件安全测试

1 范围

本标准给出了证券期货行业信息系统建设过程中的软件安全测试目标及流程、软件安全测试技术、软件安全测试基本测试方法及移动应用安全测试特定测试方法。

本标准适用于指导证券期货行业市场核心机构（以下简称核心机构）、证券期货基金经营机构（以下简称经营机构）以及证券期货信息技术服务机构（以下简称服务机构）实施证券期货业计算机软件和外部信息系统的安全测试。

注1：核心机构，如证券期货交易所、证券登记结算机构、期货市场监控中心等；

注2：经营机构，如证券公司、期货公司、基金公司等；

注3：服务机构为软件开发商、信息商、服务商。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求

GB/T 25069-2010 信息安全技术术语

JR/T 0060-2010 证券期货业信息系统安全等级保护基本要求（试行）

JR/T 0067-2011 证券期货业信息系统安全等级保护测评要求（试行）

JR/T 0146-2016（所有部分） 证券期货业信息系统审计指南

JR/T 0175-2019 证券期货业软件测试规范

3 术语和定义

GB/T 25069-2010界定的以及下列术语和定义适用于本文件。

3.1

软件安全测试 software security testing

在信息系统软件产品的生命周期中，对软件产品进行检验，以验证软件产品符合安全需求和软件产品质量标准的过程。

3.2

渗透测试 penetration testing

以未经授权的动作绕过某一系统的安全机制的方式，检查数据处理系统的安全功能，以发现信息系统安全问题的手段。

[GB/T 25069-2010，定义2.3.87]

3.3

模糊测试 fuzz testing

通过向目标系统提供非预期的输入并监视异常结果来发现软件漏洞的技术。

3.4

敏感信息 sensitive information

一旦遭到泄露或修改，会对标识的信息主体造成影响的信息。

注：证券期货行业敏感信息包括客户姓名、客户详细地址、客户联系电话、客户证件号码、客户开户行及账号、会员交易情况、会员持仓数量、会员可用资金等。

3.5

移动互联网应用程序 mobile internet application

通过预装、下载等方式获取并运行在移动智能终端上、向用户提供信息服务的应用软件。

4 软件安全测试内容及流程

4.1 测试内容

软件安全测试的内容包括：

a) 确定软件的安全特性实现与预期设计一致；
b) 检测软件中潜在的漏洞和风险；
c) 检验软件产品在受到恶意攻击的情形下，依然能够继续正确运行并确保软件被在授权范围内合法使用的能力；

4.2 测试流程

4.2.1 系统分析

评估被测系统，分别从物理架构及逻辑架构的角度分析系统使用的组件、网络拓扑、系统配置与安全防御措施等信息：

a) 物理架构：根据系统所使用的组件梳理得到物理架构，包括数据库、控制组件、前端库以及通信协议等，进而了解系统的结构；
b) 逻辑架构：根据系统的业务逻辑梳理得到逻辑架构，进而了解系统内部的数据流。

4.2.2 威胁分析

根据系统分析的结果，选择合适的威胁模型，分析系统面临的主要安全威胁。风险分析应符合GB/T 20271-2006。如常见的基于数据流的威胁分析模型STRIDE，它包含六个维度（假冒、篡改、否认、信息泄露、拒绝服务和提升权限）的威胁，通常结合使用数据流关系图(DFD)来辅助STRIDE分析，将系统分解成部件，并证明每个部件都不易受相关威胁攻击。

系统分析及威胁分析完成后，应产出安全测试方案，方案内容包括系统分析阶段的物理架构、逻辑架构，以及威胁分析阶段的数据流关系图、制定的技术方案、实施方案等，报告格式可参照模板输出（参见附录A的图A.1）。

4.2.3 制定测试用例

根据威胁分析的结果编写测试用例，针对分解的每一个数据流图，对每一个数据流图元素，映射对应的威胁，编写测试用例，用例可参照模板输出（参见附录A的图A.2）。

4.2.4 测试执行

测试执行包括自动化的工具执行以及手动执行两种方式，在此过程中需要用到各种自动化或手动测试工具。对于每一个用例的测试过程，需要有对应的操作截图，如果能够获得应用程序源代码，可以进行源码方向的安全审计。

4.2.5 报告输出

软件安全测试流程各阶段的输出文档，包括如下基本内容（见表 1 所示），可根据实际需要适当裁剪，具体模板参照附录 A。

表 1 报告的基本内容

阶段	输出文档	报告的基本内容
系统分析、威胁分析	安全测试方案	包括系统分析阶段的物理架构、逻辑架构等，威胁分析阶段的数据流关系图，以及制定的技术方案、实施方案等。
制定测试用例	安全测试用例	包括测试用例标识、用例名称、前提条件、测试目的、测试步骤、期望结果、实际结果、不通过原因、执行日期等。
报告输出	安全测试报告	包括测试范围、测试环境（测试版本、软/硬件环境清单、测试周期等）、测试结论（多角度、多维度展现系统的整体安全状况）、测试执行描述（人员、测试方法等）、测试结果汇总与缺陷分析以及改善建议等。

5 软件安全测试技术

5.1 安全功能检查

通过人工检查、审核的方式对软件开发过程中涉及的安全策略、进度、技术决策（如开发模型等）进行安全功能检查。

检查内容包括文档、代码安全策略、安全要求、架构安全性等，检查的形式包括人工文件分析、访谈等。安全性测试的相关要求见 JR/T 0175-2019。

5.2 代码安全测试

通过对软件源代码进行安全扫描和审计，定位漏洞代码所在位置。

测试内容分为静态检测与动态检测，覆盖范围广、测试效率高。静态检测基于权威软件安全规范，如开放式Web应用程序安全项目（OWASP）、公共漏洞和暴露（CWE）、支付卡行业数据安全标准（PCI DSS）等，可以发现如变量未初始化、数组越界、缓冲区溢出、浮点数比较、除零等严重代码编写错误，以及其它代码规范问题。动态检测是指运行被测程序，检测内存溢出、资源泄露、进程线程异常等在代码执行时才会发现的安全问题。

5.3 漏洞扫描

通过自动化扫描方式，检测系统和应用中存在的安全漏洞。

测试内容为基于漏洞数据库或特征库，通过自动化工具扫描、探测等方法对目标系统的安全情况进行检测，发现可利用漏洞的一种安全测试技术。它能够定位漏洞准确位置，覆盖范围广。但由于自动化工具在很多情况下只是提示一种漏洞存在的可能，因此需要对结果进行人工的分析判断。

5.4 渗透测试

以攻击者视角进行的黑盒测试，从而获得对应用系统安全的主观评价。

测试内容为以未经授权的动作，主要指模拟黑客的各种攻击方法，绕过某一系统的安全机制，对主

机或网络进行攻击测试，以检查系统的安全功能，发现安全问题或风险，或者用于重现某一攻击场景。该项测试的测试结果通常真实有效且较为严重。

5.5 模糊测试

以向目标系统提供非预期输入的方式，提高应用程序的健壮性及抵御意外输入时的安全性。

测试内容主要是向被测系统提供非预期的输入，并监视系统的异常表现或故障。它充分利用机器的能力通过自动化或半自动化的方式执行，具有原理简单，易于开发适合自身系统的模糊测试工具的特点。模糊测试根据实际场景可选择是否使用工具，使用工具时包含以下过程：

a) 测试工具通过随机或是半随机的方式生成大量变异数据；
b) 测试工具将生成的变异数据通过输入方式发送给被测系统；
c) 测试工具检测并监控被测系统的状态（如是否能够响应，响应是否正确等）；
d) 测试工具根据被测系统的状态判断是否存在潜在的安全漏洞，并记录异常日志。

5.6 软件安全测试技术选择

软件测试人员可以根据不同的机构、部署环境和系统类别，选择与之相应的软件安全测试技术，见表2～表8。机构的划分遵循JR/T 0146-2016（所有部分）。

表 2 行业软件安全测试技术对应表-证券交易所

部署环境	系统类别	系统举例	安全功能检查	代码安全测试	漏洞扫描	渗透测试	模糊测试
面向专网	交易系统	核心交易行情系统、竞价撮合平台、综合业务平台、衍生品交易平台、国际互联互通平台等	√	√	√	√	√
	业务系统	业务管理系统、期权风控系统、实时监察系统、大数据平台、市场服务资料库等	√	√	√	√	
	办公系统	办公自动化（OA）系统、企业资源计划（ERP）系统、在线培训系统、人力资源（HR）系统等	√	√	√		
面向互联网	互联网服务系统	交易所网站、网下 IPO、交易参与人业务管理系统、基金业务系统、基金会员、费用收付、统一用户登录、结算管理系统（BMS）、债券业务、债券招标发行、债券监管、债券申报、金融云等	√	√	√	√	
注：“√”为必选项							

表 3　行业软件安全测试技术对应表-期货交易所

部署环境	系统类别	系统举例	安全功能检查	代码安全测试	漏洞扫描	渗透测试	模糊测试
面向专网	交易系统	核心交易系统	√	√	√	√	√
	业务系统	结算系统、业务管理系统、会员服务系统、监察实时系统、监察预警系统、资金风险评估系统、期权参数管理系统、数据查询系统等	√	√	√	√	
	办公系统	办公自动化（OA）系统、在线培训系统等	√	√	√		
面向互联网	互联网服务系统	交易所网站、电子仓单系统、场外市场、移动应用程序等	√	√	√	√	
注：“√”为必选项							

表 4　行业软件安全测试技术对应表-证券登记结算机构

部署环境	系统类别	系统举例	安全功能检查	代码安全测试	漏洞扫描	渗透测试	模糊测试
面向专网	交易系统	-					
	业务系统	证券登记结算系统、统一账户平台和基金 TA 系统	√	√	√	√	
	办公系统	办公自动化（OA）系统、企业资源计划（ERP）系统等	√	√	√		
面向互联网	互联网服务系统	官方网站、互联网在线业务平台等	√	√	√	√	
注：“√”为必选项							

表 5　行业软件安全测试技术对应表-其他核心机构

部署环境	系统类别	系统举例	安全功能检查	代码安全测试	漏洞扫描	渗透测试	模糊测试
面向专网	交易系统	-					
	业务系统	证联网业务管理平台、中央信息监管平台、期货市场统一开户系统、基金报送系统、基金校验系统、基金数据管理系统等	√	√	√	√	

表 5　行业软件安全测试技术对应表-其他核心机构（续）

部署环境	系统类别	系统举例	安全功能检查	代码安全测试	漏洞扫描	渗透测试	模糊测试
面向专网	办公系统	办公自动化（OA）系统、期货保证金监控系统、投资者查询服务系统、期货市场运行监测监控系统等	√	√	√		
面向互联网	互联网服务系统	官方网站、统一信息披露平台、基金报送系统、基金信息披露系统、标准网电子化平台、期货互联网开户云平台、指数系统等	√	√	√	√	
注：“√”为必选项							

表 6　行业软件安全测试技术对应表-证券公司

部署环境	系统类别	系统举例	安全功能检查	代码安全测试	漏洞扫描	渗透测试	模糊测试
面向专网	交易系统	柜台交易系统、集中交易系统、主经纪商（PB）业务系统、极速交易系统、公司及营业部结算系统等	√	√	√	√	√
面向专网	业务系统	经纪业务运营平台、统一账户平台、内存风控系统、呼叫中心平台、投资者服务平台、专业投资者服务平台、登记托管系统等	√	√	√	√	
	办公系统	办公自动化（OA）系统、客户关系管理（CRM）系统等	√	√	√	√	
面向互联网	互联网服务系统	公司网站、网上交易客户端、手机证券客户端等	√	√	√	√	
注：“√”为必选项							

表 7　行业软件安全测试技术对应表-基金管理公司

部署环境	系统类别	系统举例	安全功能检查	代码安全测试	漏洞扫描	渗透测试	模糊测试
面向专网	交易系统	O32 投资交易平台、场外交易平台等	√	√	√		
	业务系统	TA 系统、估值核算系统、资金清算系统等	√	√	√		

表 7　行业软件安全测试技术对应表-基金管理公司（续）

部署环境	系统类别	系统举例	安全功能检查	代码安全测试	漏洞扫描	渗透测试	模糊测试
面向专网	办公系统	办公自动化（OA）系统、客户关系管理（CRM）系统、营销服务一体化平台等	√	√	√		
面向互联网	互联网服务系统	公司网站、订单系统、移动应用程序等	√	√	√	√	√
注：“√”为必选项							

表 8　行业软件安全测试技术对应表-期货公司

部署环境	系统类别	系统举例	安全功能检查	代码安全测试	漏洞扫描	渗透测试	模糊测试
面向专网	交易系统	柜台交易系统（主席和次席）、程序化交易系统、资管平台、核心交易结算系统等	√	√	√	√	√
	业务系统	风控系统、监控系统等	√	√	√	√	
面向专网	办公系统	办公自动化（OA）系统、客户关系管理（CRM）系统等	√	√	√		
面向互联网	互联网服务系统	公司网站、交易客户端、资管平台等	√	√	√	√	
注：“√”为必选项							

6　软件安全测试基本测试方法

6.1　身份认证安全

6.1.1　测试目标

应用程序在授予访问权限之前进行了身份验证、对数据访问进行限制并且认证信息不会被绕过。

6.1.2　测试内容

若该系统安全等级为等保三级及以上或系统设计文档中明确具有身份认证功能，其应用安全应符合JR/T 0060-2010和JR/T 0067-2011，检测内容包括：

a）　服务端对用户请求等操作均进行了认证授权，认证的方式包括采用静态密码、动态口令、USBkey等；
b）　服务端与客户端使用双因子或多因子认证机制；
c）　服务端具备登录异常处理机制；
d）　服务端能够对验证码等措施的认证绕过进行防范；
e）　认证信息不会被轻易破解和篡改。

6.1.3 结果判定

若完全符合 6.1.2 测试内容，则判定应用程序符合本项测试需求，否则判定其不符合或部分符合本项测试需求。

6.2 口令安全

6.2.1 测试目标

应用程序使用了强密码策略，对用户登录有错误次数限制，在超过规定错误次数后，对用户进行锁定或冻结。

6.2.2 测试内容

检测内容包括：

a) 服务端能够对口令复杂度进行安全检测并提示；
b) 密码输入框不以明文形式显示密码；
c) 服务端对用户登录错误次数进行限制；
d) 服务端口令找回功能的密码找回凭证足够复杂、不可猜测并且不存在越权。
e) 服务端对用户登录失败进行统一提示。

6.2.3 结果判定

若完全符合 6.2.2 测试内容，则判定应用程序符合本项测试需求，否则判定其不符合或部分符合本项测试需求。

6.3 访问权限安全

6.3.1 测试目标

应用程序对用户权限进行了配置，不会发生越权行为（包括横向越权和纵向越权）。

6.3.2 测试内容

若该系统安全等级为等保三级及以上或系统设计文档中明确具有访问权限控制功能，检测内容包括：

a) 服务端具备权限配置功能，且有权限判断机制；
b) 服务端对敏感数据进行访问权限控制；
c) 服务端对每个请求 URL 进行鉴权，而非仅仅通过客户端的菜单屏蔽或者按钮不可用来限制；
d) 用户认证采用多因子认证方式，防止通过修改用户身份证明（UID）实现越权操作。

6.3.3 结果判定

若完全符合 6.3.2 测试内容，则判定应用程序符合本项测试需求，否则判定其不符合或部分符合本项测试需求。

6.4 会话管理安全

6.4.1 测试目标

应用程序在用户登录并空闲一定时间后，会对用户会话进行检测，对超时会话进行自动终止。

6.4.2 测试内容

检测内容包括：

a) 已对会话信息进行安全加密；
b) 用户登录后，身份信息不再由客户端提交，而是以服务器端会话信息中保存的身份信息为准；
c) 应用程序提供注销登录功能，注销时，会话信息随之清除；
d) 每次登录成功后变更会话标识；
e) 对用户的操作进行 token 验证，防止跨站请求伪造（CSRF）的操作。

6.4.3 结果判定

若完全符合 6.4.2 测试内容，则判定应用程序符合本项测试需求，否则判定其不符合或部分符合本项测试需求。

6.5 通信安全

6.5.1 测试目标

应用程序在处理通信过程中使用了安全的通信协议，并对传输数据采用了加密传输的机制。

6.5.2 测试内容

若该系统安全等级为等保三级及以上或系统设计文档中明确具有通信安全要求，检测内容包括：

a) 应用程序在进行通信时采用了安全通信协议，例如 SSL/TLS、IPSec 等；
b) 应用程序在进行通信时对通信数据进行加密保护；
c) 应用程序在进行通信时对通信数据进行完整性校验；
d) 应用程序对通信数字证书进行安全性校验。

6.5.3 结果判定

若完全符合 6.5.2 测试内容，则判定应用程序符合本项测试需求，否则判定其不符合或部分符合本项测试需求。

6.6 业务逻辑安全

6.6.1 测试目标

使用户按照预定的规则运行应用程序，保护业务系统免受业务安全威胁。

6.6.2 测试内容

检测内容包括：

a) 应用程序业务数据不可被篡改；
b) 应用程序业务逻辑工作流不可被打破；
c) 应用程序不允许用户上传业务逻辑允许以外的文件类型的文件；
d) 应用程序业务接口调用足够安全。

6.6.3 结果判定

若完全符合 6.6.2 测试内容，则判定应用程序符合本项测试需求，否则判定其不符合或部分符合本项测试需求。

6.7 输入数据安全

6.7.1 测试目标

应用程序的所有用户输入都应该经过验证，并且所有的输入都是合法的、期望的类型和方式。

6.7.2 测试内容

若该系统安全等级为等保三级及以上或系统设计文档中明确具有输入数据安全要求，检测内容包括：

a) 应用程序不存在 SQL 注入漏洞；
b) 应用程序不存在跨站脚本攻击(XSS)漏洞；
c) 应用程序不存在 XXE 漏洞；
d) 应用程序不存在命令执行漏洞；
e) 应用程序不存在文件包含漏洞；
f) 应用程序不存在 HTTP 代码注入漏洞；
g) 应用程序具备特殊字符过滤机制。

6.7.3 结果判定

若完全符合 6.7.2 测试内容，则判定应用程序符合本项测试需求，否则判定其不符合或部分符合本项测试需求。

6.8 存储数据安全

6.8.1 测试目标

客户端程序对存储在客户端的敏感数据进行了加密保护。

6.8.2 测试内容

检测内容包括：

a) 客户端对本地存储的数据进行加密保护（包括数字证书文件）；
b) 客户端对本地存储的数据进行完整性校验；
c) 客户端未在本地存储用户身份认证等敏感信息。

6.8.3 结果判定

若完全符合 6.8.2 测试内容，则判定应用程序符合本项测试需求，否则判定其不符合或部分符合本项测试需求。

6.9 提示信息安全

6.9.1 测试目标

服务器在处理登录操作时不会针对认证错误的情况提示准确详实的信息。

6.9.2 测试内容

服务端对客户端错误请求引起的提示信息进行模糊处理。

6.9.3 结果判定

若完全符合 6.9.2 测试内容，则判定应用程序符合本项测试需求，否则判定其不符合或部分符合本项测试需求。

6.10 日志数据安全

6.10.1 测试目标

客户端程序中没有调用调试日志函数，不会暴露客户端代码逻辑信息。

6.10.2 测试内容

检测内容包括：

a) 客户端对日志数据进行加密保护；
b) 客户端不在本地存储与应用程序运行逻辑相关的日志数据与调试信息；
c) 应用程序服务端信息只存放于服务器端日志中。

6.10.3 结果判定

若完全符合 6.10.2 测试内容，则判定应用程序符合本项测试需求，否则判定其不符合或部分符合本项测试需求。

6.11 算法安全

6.11.1 测试目标

客户端程序中使用加密算法时没有使用不安全的加密算法或不安全的加密模式。

6.11.2 测试内容

检测内容包括：

a) 客户端采用国家管理部门认可的加解密算法，例如 SM2、SM3、SM4 算法等；
b) 客户端采用国家管理部门认可的加解密算法的安全加密模式。

6.11.3 结果判定

若完全符合 6.11.2 测试内容，则判定应用程序符合本项测试需求，否则判定其不符合或部分符合本项测试需求。

6.12 安全审计

6.12.1 测试目标

应用程序提供安全审计功能，能够记录和审查用户操作应用程序的过程，对已出现的破坏事件做出评估，并提供有效的灾难恢复和追究责任的依据。

6.12.2 测试内容

检测内容包括：

a) 应用程序提供安全审计功能，对用户的注册、登录、关键业务操作等行为进行日志记录；
b) 应用程序对安全审计记录及审计策略设置必要的访问控制，禁止未授权的删除、修改或覆盖等。

6.12.3 结果判定

若完全符合 6.12.2 测试内容，则判定应用程序符合本项测试需求，否则判定其不符合或部分符合本项测试需求。

6.13 配置安全

6.13.1 测试目标

运行应用程序的服务器是安全的。

6.13.2 测试内容

检测内容包括：

a) 服务器和中间件不存在已知的安全漏洞；
b) 服务器和中间件不存在弱口令；
c) 服务器未开启不必要的端口和服务；
d) 服务器未打开不必要的 HTTP 方法；
e) 服务器和中间件满足权限和功能最小化原则；
f) 服务器已安装最新安全补丁；
g) 服务器和中间件已开启日志审计功能。

6.13.3 结果判定

若完全符合 6.13.2 测试内容，则判定应用程序符合本项测试需求，否则判定其不符合或部分符合本项测试需求。

6.14 拒绝服务

6.14.1 测试目标

网络中所有合法用户均能正常连接到服务器，不存在拒绝服务(DoS)漏洞。

6.14.2 测试内容

检测内容包括：

a) 应用程序在面对极大量网络流量攻击请求时，不会因网络流量超大而无法提供服务；
b) 应用程序不会因为某个服务器资源耗尽而无法提供服务。

6.14.3 结果判定

若完全符合 6.14.2 测试内容，则判定应用程序符合本项测试需求，否则判定其不符合或部分符合本项测试需求。

6.15 源代码安全

6.15.1 测试目标

客户端代码不存在源代码被反编译而泄露的风险。

6.15.2 测试内容

检测内容包括：

a) 客户端的源代码已通过防动态调试、代码混淆等处理，以防止反编译或逆向分析，确保程序逻辑的机密性；
b) 客户端具备源代码完整性校验能力；
c) 客户端能够对签名信息进行安全校验。

6.15.3 结果判定

若完全符合 6.15.2 测试内容，则判定应用程序符合本项测试需求，否则判定其不符合或部分符合本项测试需求。

6.16 源代码数据安全

6.16.1 测试目标

应用程序代码内部不包含残留测试信息，例如内网URL地址、测试账号等。

6.16.2 测试内容

检测内容包括：
a) 应用程序源代码中无冗余代码或注释代码，比如开发人员信息、调试信息等；
b) 程序源代码不包含残留测试信息，例如内网 URL 地址等。

6.16.3 结果判定

若完全符合 6.16.2 测试内容，则判定应用程序符合本项测试需求，否则判定其不符合或部分符合本项测试需求。

6.17 架构安全

6.17.1 测试目标

应用程序使用的框架安全，不存在已知的漏洞。

6.17.2 测试内容

检测内容包括：
a) 应用程序使用的框架，如 Spring、Hibernate、jQuery 等，不存在已知的漏洞；
b) 应用程序使用的第三方组件，如 FCKEditor 编辑器等，不存在已知的漏洞。

6.17.3 结果判定

若完全符合 6.17.2 测试内容，则判定应用程序符合本项测试需求，否则判定其不符合或部分符合本项测试需求。

7 移动应用安全测试特定测试方法

7.1 运行环境安全

7.1.1 测试目标

移动应用程序拥有常规的运行环境检查机制，以确保移动应用程序在安全的环境下正常稳定运行。

7.1.2 测试内容

检测内容包括：

a) 移动应用客户端能够对运行环境进行安全检测，例如限制移动应用在 root 或越狱等环境下使用；
b) 移动应用客户端具有版本检测机制，提供版本更新功能；
c) 移动应用程序具有异常处理安全机制，确保客户端正常稳定运行。

7.1.3 结果判定

若完全符合 7.1.2 测试内容，则判定应用程序符合本项测试需求，否则判定其不符合或部分符合本项测试需求。

7.2 安装卸载安全

7.2.1 测试目标

移动应用程序的安装需得到明确授权，且安装过程中不应破坏移动终端环境。卸载时，应能删除由其生成的数据和信息。

7.2.2 测试内容

检测内容包括：

a) 移动应用程序安装时提示用户对其使用的终端资源（包含通信资源和外设接口）和终端数据进行确认；
b) 移动应用程序安装和使用过程中的缓存数据能完全删除，且在删除用户使用过程中生成的数据时进行提示；
c) 移动应用程序卸载后不应影响终端操作系统和其他应用软件的功能。

7.2.3 结果判定

若完全符合 7.2.2 测试内容，则判定应用程序符合本项测试需求，否则判定其不符合或部分符合本项测试需求。

7.3 组件安全

7.3.1 测试目标

移动应用程序中的组件未开启导出权限，不存在导出的风险。

7.3.2 测试内容

检测内容包括：

a) 移动应用客户端对组件权限进行限制，避免第三方移动应用随意调用组件内容；
b) 移动应用客户端对组件进行安全配置，避免发生劫持组件的安全问题；
c) 移动应用客户端的 webview 组件不存在远程代码执行漏洞；
d) 移动应用客户端的 Intent 组件不存在隐式调用的风险。

7.3.3 结果判定

若完全符合 7.3.2 测试内容，则判定应用程序符合本项测试需求，否则判定其不符合或部分符合本项测试需求。

7.4 权限安全

7.4.1 测试目标

移动应用程序使用了合理的权限，且仅使用必需的最小权限。

7.4.2 测试内容

检测内容包括：

a) 移动应用客户端已删除多余的权限配置，避免冗余权限的滥用；

b) 移动应用客户端具备对权限申请模块进行完整性校验的功能。

7.4.3 结果判定

若完全符合 7.4.2 测试内容，则判定应用程序符合本项测试需求，否则判定其不符合或部分符合本项测试需求。

7.5 第三方库安全

7.5.1 测试目标

移动应用程序安装包中的动态链接库（so）文件不可被破解读取。

7.5.2 测试内容

检测内容包括：

a) 移动应用客户端中的 so 文件不可被破解读取；

b) 移动应用客户端对第三方库进行完整性校验。

7.5.3 结果判定

若完全符合 7.5.2 测试内容，则判定应用程序符合本项测试需求，否则判定其不符合或部分符合本项测试需求。

7.6 安装包安全

7.6.1 测试目标

移动应用程序的源代码、资源文件、配置文件等被篡改后，不可以重新打包并正常运行。

7.6.2 测试内容

测试要求检测移动应用客户端的源代码、资源文件、配置文件等被篡改后，不可以重新打包并正常运行。

7.6.3 结果判定

若完全符合7.6.2测试内容，则判定应用程序符合本项测试需求，否则判定其不符合或部分符合本项测试需求。

附 录 A
（资料性附录）
软件安全测试模板

A.1.软件安全测试方案

软件安全测试方案模板如图A.1所示：

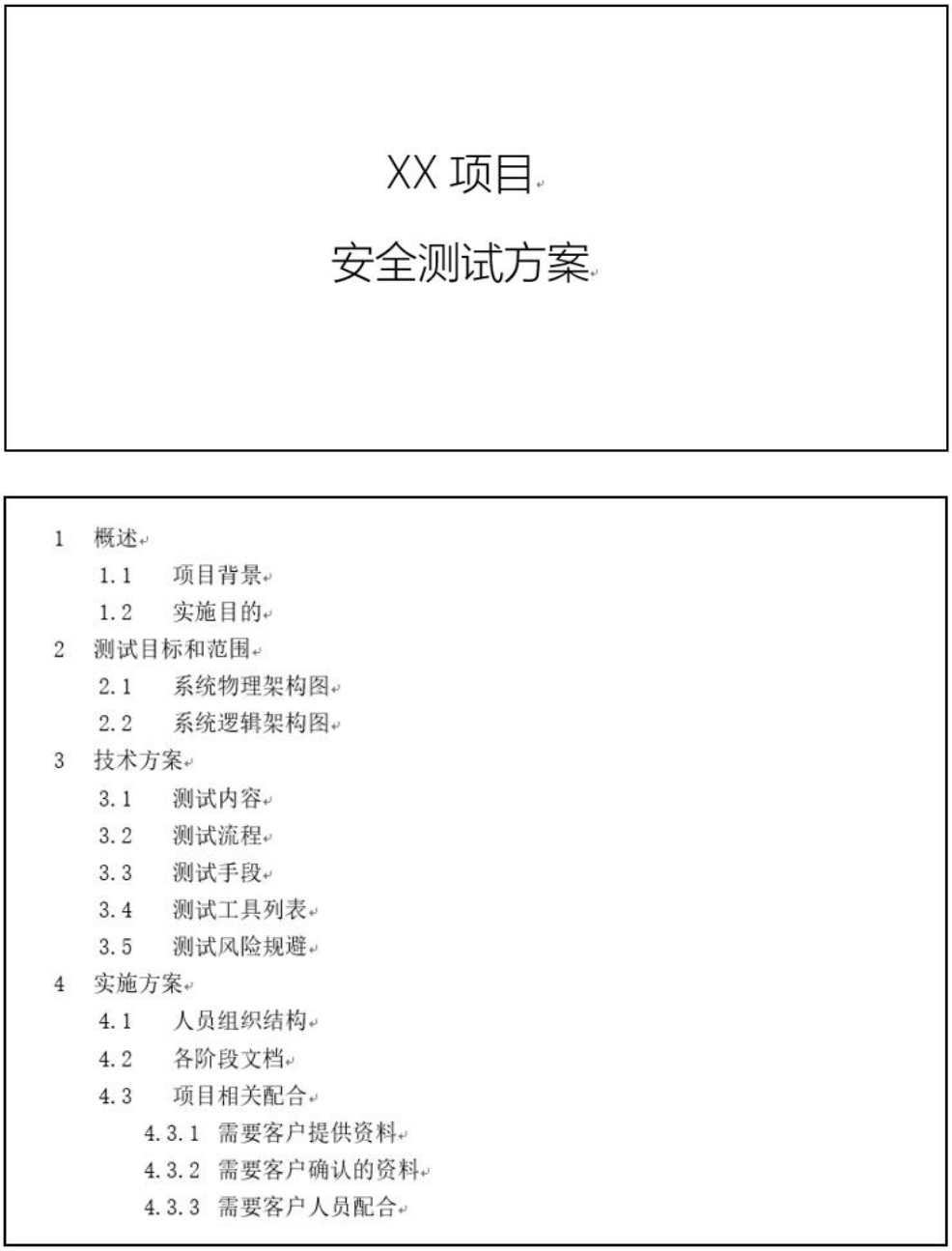

图 A.1 软件安全测试方案模板

A.2.软件安全测试用例

软件安全测试用例模板如图A.2所示：

测试用例ID	用例名称	测试目的描述	前提条件	测试步骤概述	期望结果	实际结果	Pass/Fail/NT	测试人员	测试日期	备注

图 A.2　软件安全测试用例模板

A.3.软件安全测试报告

软件安全测试报告模板如图A.3所示：

XX 项目

安全测试总结报告

图 A.3　软件安全测试报告模板