ICS 35.080
L 77

DL

中华人民共和国电力行业标准

DL / T 2031 — 2019

电力移动应用软件测试规范

Test specification for power mobile application software

2019-06-04发布　　2019-10-01实施

国家能源局　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009《标准化工作导则　第 1 部分：标准的结构和编写》给出的规则起草。

本标准由中国电力企业联合会提出。

本标准由电力行业信息标准化技术委员会（DL/TC 27）归口。

本标准起草单位：中国电力科学研究院有限公司、国家电网有限公司、中国南方电网有限责任公司、南瑞集团有限公司、国网山东省电力有限公司。

本标准主要起草人：汪洋、王志英、丁慧霞、汤国龙、程磊、赵莹、颉月平、方帅、王智慧、张庚、滕玲、李哲、陈相舟、董慧博、董灿、冯国聪、胡牧、蒋厚明、胡昊伟、王勇、邓昊、卢立生、李健。

本标准为首次发布。

本标准在执行过程中的意见或建议反馈至中国电力企业联合会标准化管理中心（北京市白广路二条一号，100761）。

电力移动应用软件测试规范

1 范围

本标准规定了电力移动应用软件在系统测试阶段的测试环境、测试方法和测试过程。

本标准适用于电力行业移动应用软件的系统测试环节，其他软件系统可参照执行。

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 15532 计算机软件测试规范

GB 17859 计算机信息系统 安全保护等级划分准则

GB/T 18336 信息技术 安全技术 信息技术安全评估准则

GB/T 22239 信息安全技术 信息系统安全等级保护基本要求

GB/T 25069—2010 信息安全技术 术语

GB/T 34975 信息安全技术 移动智能终端应用软件安全技术和测试评价方法

YD/T 2558 基于祖冲之算法的 LTE 终端和网络设备安全技术要求

3 术语和定义

GB/T 15532、GB/T 18336、GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

移动应用软件 mobile application

可独立运行在移动终端系统上的应用，拥有系统本身独立的应用服务器、数据库服务器，不借用其他软件或平台作为入口，可独立发布、安装、运行、卸载等。

3.2

黑盒测试 black box testing

在完全不考虑程序内部结构和内部特性的情况下，检查程序功能是否按照需求规格说明书的规定正常使用，程序是否能适当地接收输入数据而产生正确的输出信息。

3.3

交叉事件测试 cross event test

一个功能正在执行过程中，同时另外一个事件或操作对该过程进行干扰的测试。

3.4

系统完整性 system integrity

系统能够以不受损害的方式执行其预定功能，避免对系统故意的或意外的未授权操纵的特性。

[GB/T 25069—2010，定义 2.1.49]

3.5

数据完整性 data integrity

数据没有遭受以未授权方式所做的更改或破坏的特性。

[GB/T 25069—2010，定义 2.1.36]

3.6

保密性　confidentiality

使信息不泄露给未授权的个人、实体、进程，或不被其利用的特性。

［GB/T 25069—2010，定义 2.1.1］

3.7

加密技术　encryption technology

采用数学方法对原始信息进行再组织，使得加密后在网络上公开传输的内容对于非法接受者来说成为无意义的文字的安全保密手段。

3.8

组件　component

对数据和方法的简单封装，本标准中包括组成安卓应用程序的组件，即 Activities（活动）、Service（服务）、Content Provider（内容提供器）、Broadcast Receiver（广播接收器）、Intent（意图）等。

3.9

活动组件　acitivities component

安卓应用程序的组件之一，提供一个屏幕，负责与用户交互。

3.10

服务组件　service

安卓应用程序的组件之一，通常在后台运行，主要用于在后台处理一些耗时的逻辑，或者执行某些需要长期运行的任务。

3.11

内容提供器　content provider

安卓应用程序的组件之一，用来管理和共享应用程序的数据库。

3.12

广播接收器　broadcast receiver

安卓应用程序的组件之一，用于接收并响应广播通知。

3.13

意图组件　intent

安卓应用程序的组件之一，简单的消息传递框架。

3.14

网络视图　webview

移动平台提供给移动应用软件使用的软件开发工具包（SDK）封装好的组件，主要作为网络浏览器。

3.15

代码混淆　code obfuscation

将计算机程序的代码转换成一种功能上等价，但是难于阅读和理解的形式的行为，目的是防止软件被破解或篡改。

3.16

数字签名　digital signature

一种类似写在纸上的普通的物理签名，但是使用了公钥加密领域的技术实现，用于鉴别数字信息的方法。一套数字签名通常定义两种互补的运算，一个用于签名，另一个用于验证。

3.17

权限攻击　privilege attack

低权限程序调用高权限程序的攻击行为。

3.18

模拟器 simulator

可以在非移动平台，如 Windows 等环境下通过软件模拟移动平台系统的软件。

4 缩略语

下列缩略语适用于本文件。

ANR：应用程序无响应（application not responding）

API：应用程序编程接口（application programming interface）

FPS：画面每秒传输帧数（frames per second）

IPsec：Internet 协议安全性（internet protocol security）

SSL：安全套接层（secure sockets layer）

TLS：传输层安全（transport layer security）

5 测试环境

测试环境应包括测试运行环境和测试工具环境。测试运行环境一般应符合电力移动应用的系统规格说明书和相关设计文档的要求，通常是开发环境或模拟仿真环境，移动应用软件测试环境一般包括客户端、服务端、测试通信网络，测试通信网络应使用适用于测试的安全无线接入设备。电力移动应用的网络要求应遵循相关电力移动应用设计说明文档，组建相应测试仿真网络环境，并在仿真网络环境下开展测试，测试使用的通信网络设备要求见 YD/T 2558。测试工具一般要求是经过认可的工具。测试环境的要求见 GB/T 15532。

6 测试方法

主要涉及以下两种方法：

a） 黑盒测试：该方法的说明参见附录 A。

b） 渗透测试：利用攻击工具或通过人工操作的方式攻击移动应用系统，验证其是否存在安全漏洞，参见附录 B。

7 功能测试

7.1 功能性测试

7.1.1 测试项

功能性测试应对照移动应用设计说明中的功能点，逐项对其进行测试用例设计，测试用例的设计应满足：

a） 移动应用的每个功能特性应被一个或多个正常测试用例和一个或多个被认可的异常测试用例所覆盖；

b） 测试用例的输入应至少包括有效等价类值、无效等价类值和边界数据值；

c） 逐项测试移动应用设计说明规定的功能特性；

d） 测试移动应用配置项之间及软件配置项与硬件之间的接口；

e） 测试移动应用输出及其格式；

f） 测试运行条件在边界状态和异常状态下。

7.1.2 测试过程

下列测试过程适用于功能性测试：

a） 根据需求规格说明书、概要设计等相关软件设计说明，分析并拆分移动应用功能点；
b） 根据拆分的移动应用功能点，采用“黑盒测试”方法逐一设计测试用例，测试用例应覆盖所有功能点，覆盖率应达到100%；
c） 根据移动应用相关设计说明，编制每条测试用例的执行步骤、测试结果；
d） 执行每条测试用例；
e） 检验执行结果是否满足测试用例预期结果；
f） 根据执行结果填写执行记录和缺陷报告。

7.1.3 测试结果

功能性测试结果，应满足下列要求：
a） 通过所有功能性测试用例；
b） 移动应用应满足所有经评审后的设计说明规定文档中的功能要求。

7.2 交叉事件测试

7.2.1 测试项

从交叉事件测试方面考虑，应测试：
a） 移动应用在填写表单时中断后的恢复情况；
b） 移动终端操作系统，在多个移动应用同时运行时是否影响被测移动应用正常功能；
c） 移动应用运行时前后台切换、拨打接听电话、发送接收信息或邮件是否影响正常功能；
d） 移动应用在调用相机、定位功能、语音交互等功能并返回移动应用后的运行情况。

7.2.2 测试过程

下列测试过程适用于交叉事件测试：
a） 使用移动应用功能时，移动终端中断移动应用运行，检查中断移动应用运行后，移动应用恢复操作情况；
b） 使用移动应用在调用的相机、定位功能、语音交互等功能后，移动应用恢复的正确性；
c） 移动终端操作系统中同时运行多个移动应用（含被测移动应用），检查被测移动应用的运行情况。

7.2.3 测试结果

交叉事件测试结果，应满足下列要求：
a） 移动应用中断恢复后，应保持移动应用会话；
b） 移动应用中断恢复后，操作其他功能正常无误；
c） 移动应用调用相机、定位时，应能正确跳转页面，并使用相关调用数据；
d） 移动应用调用相机切换回移动应用时，移动应用应正常运行；
e） 移动终端操作系统中同时多个移动应用运行时，被测试移动应用应正常运行，保证功能完整性。

8 非功能测试

8.1 性能（效率）测试

8.1.1 服务端性能（效率）测试

8.1.1.1 测试项

移动应用运行一段时间内，满足移动应用设计说明规定的测试场景、服务器资源、并发用户数量

的同时，应测试移动应用服务端所能承受压力的强度，包括但不限于：

a） 响应时间：服务端响应事务的平均时长。

b） 每秒处理事务数（TPS）：服务端每秒处理事务的数量。

c） 事务通过率：服务端处理事务的成功率。

d） CPU 占用率：服务端在处理事务时，服务器 CPU 占用情况。

e） 内存占用率：服务端在处理事务时，服务器内存占用情况。

f） 硬盘 I/O 读写：服务端在处理事务时，服务器硬盘读写情况。

8.1.1.2 测试过程

下列测试过程适用于服务端性能（效率）测试：

a） 模拟测试场景操作步骤，与服务器建立连接，传输数据，并能得到正确的服务器反馈；

b） 回放操作步骤，模拟并发用户操作典型移动应用场景，向服务器施加压力；

c） 统计模拟多人操作时，服务端响应能力和服务器资源占用情况。

8.1.1.3 测试结果

在满足最大并发用户数量的同时，服务端性能（效率）测试结果，应满足下列要求：

a） 响应时间应在移动应用设计说明规定的时间范围内，如移动应用设计说明未规定性能指标的，一般情况下首页访问平均响应时间不应超过 2s；移动应用登录平均响应时间不得超过 3s；执行简单查询、添加和删除业务时，平均响应时间不应超过 4s；执行复杂的综合业务（同时包括查询、添加、删除等操作请求）时，平均响应时间不应超过 6s；在执行统计业务时，月统计业务的平均响应时间不应超过 10s，年统计业务的平均响应时间不应超过 20s。

b） 每秒处理事务数（TPS）应满足移动应用设计说明规定的相关约束。

c） 事务通过率应满足移动应用设计说明规定的相关约束，一般事物失败率应小于 0.1%。

d） CPU 占用率、内存占用率、硬盘 I/O 读写应在移动应用设计说明规定的范围内，一般情况下应用服务器和数据库服务器的 CPU 平均利用率不应超过 60%，且 CPU 利用率不应连续 30s 超过 80%；应用服务器的内存平均使用率不应超过 75%，且内存使用率不应连续 60s 超过 80%。

8.1.2 客户端性能（效率）测试

8.1.2.1 测试项

移动应用在不同芯片组、分辨力、型号的移动终端上执行安装、卸载、启动、运行操作时，应测试移动应用在移动终端运行时的各方面性能数据，包括但不限于：

a） Android 移动终端：

1） 响应时间：移动应用在移动终端上安装、启动、运行、卸载的响应时长。

2） CPU 占用率：移动应用运行一定时间内占用移动终端的 CPU 的平均率。

3） 内存占用率：移动应用运行一定时间内占用移动终端的内存的平均率。

4） FPS 渲染：移动应用在移动终端运行一定时间内平均每秒渲染帧数。

5） 耗电量：移动应用在移动终端运行一定时间内平均耗电量。

6） 电池温度：移动应用在移动终端运行一定时间内的平均电池温度。

7） 发送、接收流量：移动应用在移动终端运行一定时间内发送和接收的平均流量数量。

b） iOS 移动终端：

1） CPU 占用率：移动应用运行一定时间内占用移动终端的 CPU 的平均率。

2） 内存占用率：移动应用运行一定时间内占用移动终端的内存的平均率。

3） 发送、接收流量：移动应用在移动终端运行一定时间内发送和接收的平均流量数量。

8.1.2.2 测试过程

下列测试过程适用于客户端性能（效率）测试：

a） 移动应用软件安装包下发至各移动终端；

b） 通过自动化技术手段，在各移动终端进行安装、启动、运行、卸载操作；

c） 查看移动应用在移动终端设备运行进程名称，根据进程名称分别记录移动应用运行占用的资源情况。

8.1.2.3 测试结果

客户端性能（效率）测试结果，应满足下列要求：

a） 生成客户端性能测试报告，显示移动应用在不同 Android 移动终端安装、启动、运行、卸载时的响应时间、CPU 占用率、内存占用率、FPS 渲染、耗电量、电池温度、发送接收流量；

b） 生成客户端性能测试报告，显示移动应用在不同 iOS 移动终端安装、启动、运行、卸载时的 CPU 占用率、内存占用率、发送接收流量；

c） 根据生成的客户端性能测试报告，提出建议性缺陷，提高移动应用在移动终端的运行效率。

8.2 兼容性测试

8.2.1 测试项

从兼容性测试方面考虑，应测试：

a） 移动应用在不同机型、不同分辨力、不同操作系统的移动终端适配性，持续运行时长不应小于 10min；

b） 移动应用在移动终端处于低内存空间、高 CPU 占用的环境下的表现。

8.2.2 测试过程

下列测试过程适用于兼容性测试：

a） 将移动应用安装包分发至不同机型、不同分辨力、不同移动操作系统版本的移动终端上，并执行安装、卸载、启动、运行等操作，分别查看移动应用在移动终端上的运行情况；

b） 利用技术手段，使测试终端设备处于低电量、低内存空间、高 CPU 占用，检测移动应用在不同极限环境下的运行情况。

8.2.3 测试结果

兼容性测试结果，应满足下列要求：

a） 生成兼容性测试报告，移动应用应适配更多移动终端，宜保证本年度市场占有率前三位的 Android 移动终端不出现闪退、卡顿、ANR、Crash 等问题，iOS 类移动应用宜保证 iOS 移动终端上正确运行且不出现任何问题。对于移动应用不适配本年度市场占有率前三位的 Android 移动终端的情况，提出严重缺陷；对于移动应用不适配其他 Android 移动终端的情况，提出建议或一般缺陷。对于 iOS 类移动应用不适配 iOS 移动终端的情况，提出严重缺陷；移动应用应适配专控智能移动终端，对于移动应用不适配专控智能移动终端的情况，提出严重缺陷。

b） 移动应用宜在低内存空间、高 CPU 占用的移动终端上稳定运行，移动应用应避免因移动终端的低内存空间、高 CPU 占用原因出现问题，应具备清理移动终端缓存或提示用户手动清理移

动终端缓存的机制。

8.3 易用性测试

8.3.1 测试项

从易用性方面考虑，可测试：

a） 易理解性，包括但不限于用户手册易理解、移动应用界面易理解、移动应用演示易理解、输入输出含义易理解。

b） 易学习性，包括但不限于用户手册易学习、培训手册易学习、移动应用系统文档易学习。

c） 易操作性，包括但不限于表单各字段填写校验、移动应用提示语、移动应用页面风格规范性、键盘快捷键支持情况。

d） 吸引性，包括但不限于移动应用页面元素。

8.3.2 测试过程

下列测试过程适用于易用性测试：

a） 查看用户手册内容，操作移动应用过程中查看页面布局，查看输入输出项的易理解性；

b） 查看用户手册、培训手册、移动应用系统文档，查看文档能否帮助用户学习操作；

c） 检测过程对表单输入边界值外的数据，查看移动应用所有提示语及移动应用页面风格一致性，是否能使用键盘快捷键；

d） 检测过程中查看移动应用页面所有的元素是否美观，具备吸引性。

8.3.3 测试结果

易用性测试结果，应满足下列要求：

a） 用户手册中的术语、图形、背景信息、移动应用帮助应有助于理解移动应用操作，移动应用界面、排版简单易懂，演示应充分、易识别、易理解，界面的输入、输出格式和含义应具备易理解性，符合电力行业移动应用界面要求；

b） 用户手册、培训手册、移动应用系统文档应具备有效性、一致性，易定位；

c） 移动应用内的各输入项应提供校验机制，提示信息友好，界面、字体风格统一易识别，支持键盘快捷键输入；

d） 移动应用内的所有界面元素应保持一定比例，界面美观程度应符合相关电力行业移动应用界面的管理要求。

8.4 可靠性测试

8.4.1 测试项

从可靠性测试方面考虑，可测试：

a） 容错性，包括但不限于用户误操作的处理方式、误操作后的数据处理情况、误操作后移动应用的运行情况。

b） 成熟度，包括但不限于检测期间内出现的故障、纠正故障的数量。

c） 易恢复性，包括但不限于出现移动应用系统宕机和服务停止时的恢复情况。

d） 稳定性，包括但不限于：

1） 服务端承受最大并发数量持续运行 4h；

2） 移动应用在不同机型、不同分辨力、不同操作系统的移动终端上持续运行不少于 20min。

8.4.2 测试过程

下列测试过程适用于可靠性测试：

a） 移动应用操作过程中出现误操作，包括填写表单超出限制范围，违反正确业务逻辑等；
b） 记录检测过程中移动应用出现的故障及故障纠正数量；
c） 当出现移动应用宕机及服务停止时，记录移动应用系统恢复运行的时长，恢复后是否能正常运行，数据是否丢失；
d） 在满足移动应用最大并发数量且在选定好的测试场景下，持续对服务端进行业务请求，查看服务端运行情况；
e） 移动应用在多台移动终端上，通过自动化测试手段持续运行，查看移动应用运行情况。

8.4.3 测试结果

可靠性测试结果，应满足下列要求：

a） 移动应用应具备屏蔽用户误操作，并提供错误原因和纠正信息，输入错误数据或错误操作时，移动应用系统不崩溃、不异常退出、不丢失数据；
b） 检测过程中出现的移动应用故障应能及时解决，解决后不再出现该故障；
c） 检测期间模拟真实用户操作，移动应用系统因业务压力导致宕机或服务停止时，恢复时间不应大于 1h；
d） 服务端在最大并发数量持续运行 4h 期间，不应出现宕机或服务停止，移动应用系统应保持稳定运行，响应时间、每秒处理事务次数、事务通过率、CPU 占用率、内存占用率、I/O 读写应在移动应用系统设计说明规定的范围内；
e） 移动应用应兼容本年度市场占有率前三位的 Android 移动终端并能稳定运行，不出现任何问题，iOS 类移动应用全部兼容 iOS 移动终端。

8.5 可维护性测试

8.5.1 测试项

从可维护性测试方面考虑，可测试：

a） 易分析性，包括但不限于自我诊断能力、日志输出、日志级别配置。
b） 易配置性，包括但不限于图形页面配置、权限粒度。
c） 易修改性，包括但不限于变更服务手段。
d） 易测试性，包括但不限于内置测试功能、测试工具支持。

8.5.2 测试过程

下列测试过程适用于可维护性测试：

a） 查看服务端日志，检测移动应用分析诊断能力。
b） 查看移动应用图形化页面及权限配置页面，检测移动应用可配置能力。
c） 查看移动应用配置参数元文件，检测移动应用修改能力。
d） 使用主流测试工作，检测移动应用对主流测试工具的支持。

8.5.3 测试结果

可维护性测试结果，应满足下列要求：

a） 移动应用应具备完善的日志和自我诊断能力，提供多种日志输出，包括运行日志、错误日志、

登录日志等，日志格式统一，日志级别可配置；

b） 提供图形化配置页面，尽量避免对数据库、配置文件直接进行操作，缩小权限粒度，应拥有权限配置页面，明确各权限范围；

c） 当移动应用出现异常或故障时，移动应用应提供及时变更服务手段，可利用参数及时变更移动应用软件，变更后能及时反馈到移动应用；

d） 移动应用应支持主流测试工具，提供一定的内置测试功能。

8.6 可移植性测试

8.6.1 测试项

从可移植性测试方面考虑：可测试：

a） 适从性，包括但不限于对移动应用服务端元组文件的修改、多环境安装部署、多环境正确运行；

b） 易安装性，包括但不限于主流安装模式、根据文档安装、自定义安装、卸载重新安装；

c） 共存性，包括但不限于与其他软件共存。

8.6.2 测试过程

下列测试过程适用于可移植性测试：

a） 在多操作系统环境下安装部署移动应用服务端，检测移动应用运行情况；

b） 使用多种模式安装，包括服务端和移动终端；

c） 安装完成是否影响其他移动应用的正常运行。

8.6.3 测试结果

可移植性测试结果，应满足下列要求：

a） 移动应用元组件修改且配置正确情况下，移动应用能正常运行；

b） 部署在不同操作系统情况下，移动应用能正常运行；

c） 移动应用应使用主流的安装模式，可根据安装文档或自定义安装部署，包括服务端和移动终端；

d） 移动应用卸载后重新安装，可正常运行，无任何残留数据，无故障；

e） 移动应用正确安装部署后，应与移动终端操作系统的其他移动应用共存，无其他排异反应。

8.7 用户文档集检查

8.7.1 测试项

从用户文档集查检方面考虑，可测试：

a） 文档的完备性，包括但不限于移动应用安装所需信息、产品描述所有功能、移动应用维护所需信息、用户手册完整；

b） 文档的一致性，包括但不限于测试移动应用时对照文档准确性、文档与文档间的描述一致性、文档与文档间互不矛盾且术语一致；

c） 文档质量，包括但不限于符合文档编写规范且覆盖所有功能点、关键功能点应有图文说明。

8.7.2 测试过程

采用文档查阅，与实际移动应用操作对照，检查文档完备性、一致性及文档质量。

8.7.3 测试结果

用户文档集检查结果，应满足下列要求：

a） 文档应描述移动应用生命周期内的所有信息；
b） 文档与移动应用应保持一致，互不矛盾，文档间不能存在冲突；
c） 文档编写应符合相应编写规范，所述关键内容，应附图文说明。

9 安全测试

9.1 移动应用服务端

移动应用服务端应遵照 GB 17859，划分系统安全定级后，依照 GB/T 22239，对移动应用服务端应遵循的安全检测项逐一进行检测，以确保服务端安全性。

9.2 移动应用客户端

9.2.1 综述

移动应用客户端的测试内容包括安全功能测试、渗透测试和代码安全检测，其中安全功能根据其依托的操作系统分为 Android 版和 iOS 版，应遵循 GB/T 34975 的测试要求。安全测试根据对移动应用系统的危害程度，将检测项分为高风险项、中风险项和低风险项。

9.2.2 安全功能

9.2.2.1 用户鉴别

9.2.2.1.1 测试项

用户鉴别的测试项同时适用于 Android 版和 iOS 版，具体如下：
a） 应具备身份鉴别机制（中风险）；
b） 应具备鉴别失败处理机制（高风险）；
c） 鉴别失败时应具备混淆提示机制（中风险）；
d） 应具备多重鉴别机制（低风险）；
e） 与服务端通信验证时应具备双向鉴别机制（低风险）；
f） 应对关键操作采用短信验证码机制，且验证码的长度和有效期满足要求（中风险）；
g） 设置或修改口令时应禁止用户口令与用户名相同或包含用户名（中风险）；
h） 设置或修改口令时应具备复杂度检查机制（中风险）。

9.2.2.1.2 测试过程

下列测试过程适用于用户鉴别：
a） 检测移动应用启动时是否对登录用户进行身份标识和鉴别，具体措施有哪些；
b） 检测移动应用是否具有鉴别失败处理功能，是如何进行处理的（如登录失败次数超过设定值，系统自动退出等），是否可绕过；
c） 检测移动应用在鉴别失败时是否给出提示，提示内容是什么；
d） 检测移动应用是否采用了两个及两个以上身份鉴别技术的组合来进行身份鉴别（如用户名/口令、数字证书体系、硬件令牌、生物特征、一次性动态口令中的任意两个组合）；
e） 检测移动应用是否对与服务端通信时是采用何种措施相互鉴别的（如挑战应答）；
f） 检测移动应用对关键操作（如临时账户登录、用户注册、密码修改、支付确认等）是否采用短信验证码机制，是如何实现的，采用何种措施防止被冒用（如设定验证码长度、有效期等）；
g） 检测用户设置或修改口令时，用户口令与用户名是否可相同或包含用户名；

h） 检测用户设置或修改口令时，采取何种措施防止身份鉴别信息被冒用（如复杂性混有大、小写字母、数字和特殊字符，设定口令长度限制等）。

9.2.2.1.3 测试结果

用户鉴别测试结果，应满足下列要求：

a） 移动应用至少应达到以用户名+静态口令的认证强度对登录用户进行身份鉴别；
b） 移动应用应对 24h 内连续登录失败次数达到设定值（应在 1 次～10 次之内）的用户账号进行锁定，至少锁定 20min 或由授权的管理员解锁，且不可绕过；
c） 移动应用登录失败时应采用混淆提示，防止用户名或口令泄露；
d） 移动应用应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；
e） 移动应用与服务端通信时应通过证书或其他方式进行双向鉴别验证；
f） 移动应用对关键操作应采用短信验证码机制，验证码口令长度至少为 6 位，有效期最长 6min，且不包含敏感信息；
g） 移动应用应禁止用户口令与用户名相同或包含用户名；
h） 移动应用应限制用户口令长度不小于 8 位字符，应为大写字母、小写字母、数字、特殊字符中三种或三种以上的组合。

9.2.2.2 会话安全

9.2.2.2.1 测试项

会话安全的测试项同时适用于 Android 版和 iOS 版，具体如下：

a） 应具备会话超时机制，会话超时后应重新进行身份鉴别（中风险）；
b） 移动应用在退出登录后，应禁止通过原会话向服务器发起会话连接（高风险）；
c） 移动应用在未关闭的情况下，从后台唤醒时应重新进行身份鉴别（低风险）。

9.2.2.2.2 测试过程

下列测试过程适用于会话安全：

a） 检测用户登录后停止活动一段时间，是否可限制用户会话非活动的终止时间，如何进行限制；
b） 检测移动应用在退出登录后是否可继续操作原会话；
c） 检测移动应用在未关闭的情况下，进入后台一段时间（小于会话非活动终止时间）后，唤醒时是如何处理的。

9.2.2.2.3 测试结果

会话安全测试结果，应满足下列要求：

a） 移动应用应可限制用户会话非活动的终止时间，终止后需重新进行身份鉴别；
b） 移动应用在退出登录后，应可防止通过原会话向服务端发起连接；
c） 移动应用在未关闭情况下，默认或通过设置应可实现，进入后台（小于会话超时时间）唤醒时需重新进行身份鉴别。

9.2.2.3 软件容错

9.2.2.3.1 测试项

软件容错的测试项同时适用于 Android 版和 iOS 版，具体如下：

a） 应对通过人机接口输入的数据进行有效性和合法性验证（中风险）；

b） 在故障发生时，移动应用应能够继续提供一部分功能，确保能够实施必要的措施（中风险）。

9.2.2.3.2 测试过程

下列测试过程适用于软件容错：

a） 通过输入的不同（如数据格式或长度等符合、不符合软件设定的要求），验证系统人机接口是否有保证移动应用具有容错能力的措施，具体措施有哪些，措施是否有效；

b） 检测移动应用在发生故障（如网络中断）的情况下还能提供哪些功能。

9.2.2.3.3 测试结果

软件容错测试结果，应满足下列要求：

a） 移动应用应对通过人机接口输入的数据有效性进行检验，保证输入的数据符合系统设定的安全属性要求，且错误提示不包含敏感信息；

b） 移动应用在故障发生时应能够继续提供一部分功能，确保能够实施必要的措施。

9.2.2.4 输入输出安全

9.2.2.4.1 测试项

输入输出安全的测试项同时适用于 Android 版和 iOS 版，具体如下：

a） 移动应用应屏蔽或隐藏输入的隐私数据（中风险）；

b） 移动应用隐私数据输入过程中应采用具备防截屏机制的安全键盘（低风险）；

c） 移动应用隐私数据输出时应部分或全部屏蔽，禁止完全明文显示（中风险）。

9.2.2.4.2 测试过程

下列测试过程适用于输入输出安全：

a） 检测移动应用输入隐私数据（如密码、身份证号等）时是如何显示的；

b） 检测移动应用隐私数据输入过程是否使用安全键盘；

c） 检测移动应用的隐私数据是如何显示的。

9.2.2.4.3 测试结果

输入输出安全测试结果，应满足下列要求：

a） 移动应用输入隐私数据时应屏蔽或隐藏；

b） 移动应用隐私数据输入过程应采用安全键盘，键盘布局随机且具备防截屏机制；

c） 移动应用的隐私数据不应完全明文显示，可部分或全部屏蔽。

9.2.2.5 卸载升级

9.2.2.5.1 测试项

卸载升级的测试项同时适用于 Android 版和 iOS 版，具体如下：

a） 应确保卸载后无残留数据或残留数据中无敏感信息（中风险）；

b） 移动应用升级过程中应进行系统完整性校验（高风险）。

9.2.2.5.2 测试过程

下列测试过程适用于卸载升级：

a） 尝试卸载移动应用，查看卸载后是否存在移动应用的残留数据；
b） 尝试进行移动应用升级，查看升级过程能否替换升级包，升级包是如何进行校验的。

9.2.2.5.3 测试结果

卸载升级测试结果，应满足下列要求：
a） 移动应用应确保卸载后无残留数据，或残留数据中无敏感信息；
b） 移动应用升级过程应进行系统完整性校验，防止升级文件被篡改。

9.2.2.6 数据存储

9.2.2.6.1 测试项

数据存储的测试项同时适用于 Android 版和 iOS 版，具体如下：
a） 应对本地存储的隐私数据进行加密处理（高风险）；
b） 应将本地存储的数据存储在应用程序本身目录下（中风险）。

9.2.2.6.2 测试过程

下列测试过程适用于数据存储：
a） 查看移动应用隐私数据是否存储，是否采用加密或其他保护措施实现存储保密性；
b） 查看移动应用隐私数据的存储位置是什么。

9.2.2.6.3 测试结果

数据存储测试结果，应满足下列要求：
a） 移动应用应采取加密技术存储隐私数据；
b） 移动应用的隐私数据应存储在应用程序本身目录下。

9.2.2.7 组件安全

9.2.2.7.1 测试项

组件安全的测试项仅适用于 Android 版，具体如下：
a） 基于 Android 开发的移动应用应对 Activity、Broadcast Receiver、Service、Content Provider、Intent 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（中风险）；
b） 基于 Android 开发的移动应用应对 Activity、Broadcast Receiver、Service、Content Provider、Intent 组件进行安全配置，避免发生劫持组件的安全问题（高风险）；
c） 基于 Android 开发的移动应用应对 Activity、Broadcast Receiver、Service、Content Provider 组件进行安全设置，避免拒绝服务攻击漏洞（高风险）；
d） 基于 Android 开发的移动应用应对 webview 组件进行安全设置，避免远程代码执行漏洞（高风险）。

9.2.2.7.2 测试过程

下列测试过程适用于组件安全：
a） 检测移动应用的 Activity、Broadcast Receiver、Service、Content Provider、Intent 组件是否对权限进行限制，验证限制措施是否有效；
b） 检测移动应用的 Activity 组件是否有防劫持限制措施，验证限制措施是否有效；

c） 检测移动应用的 Activity、Broadcast Receiver、Service、Content Provider 从 Intent 获取数据时是否进行有效性校验；
d） 检测移动应用的 webview 组件是否调用不安全的方法。

9.2.2.7.3 测试结果

组件安全测试结果，应满足下列要求：
a） 移动应用应对 Activity、Broadcast Receiver、Service、Content Provider、Intent 组件进行权限限制，防止其被攻击；
b） 移动应用应对 Activity 组件进行安全配置，防止其被劫持；
c） 移动应用应对 Activity、Broadcast Receiver、Service、Content Provider 组件应对从 Intent 获取的数据进行有效性校验，避免拒绝服务攻击漏洞；
d） 移动应用应对 webview 组件进行安全设置，避免远程代码执行漏洞。

9.2.2.8 反编译

9.2.2.8.1 测试项

反编译的测试项仅适用于 Android 版，具体如下：
a） 基于 Android 开发的移动应用的源代码应进行混淆处理（中风险）；
b） 基于 Android 开发的移动应用应对其完整性进行安全校验（高风险）；
c） 基于 Android 开发的移动应用应对签名信息进行安全校验（高风险）；
d） 基于 Android 开发的移动应用关键代码应不可被反编译（高风险）；
e） 基于 Android 开发的移动应用 so 文件应不可被破解（低风险）。

9.2.2.8.2 测试过程

下列测试过程适用于反编译：
a） 检测移动应用安装包的源代码是否可读；
b） 尝试对移动应用进行重新编译打包并安装；
c） 尝试对移动应用进行重新签名；
d） 检测移动应用被反编译后是否可读取关键代码；
e） 检测移动应用被反编译后，so 文件结构信息是否可获取。

9.2.2.8.3 测试结果

反编译测试结果，应满足下列要求：
a） 移动应用应不可被反编译或者可得到源代码但源代码已作混淆处理；
b） 移动应用运行时应对不可被重新打包或打包成功后无法正常运行；
c） 移动应用运行时应不可被重新签名或重新签名后无法正常运行；
d） 移动应用反编译后应不可读取关键源码；
e） 移动应用反编译后应不可获取 so 文件信息。

9.2.2.9 安全加固

9.2.2.9.1 测试项

安全加固的测试项中 a）项适用于 Android 版，b）项适用于 iOS 版，具体如下：

a） 基于 Android 开发的移动应用应进行防逆向、防篡改安全措施的保护（中风险）；
b） 基于 iOS 开发的移动应用应进行防逆向、防篡改安全措施的保护（低风险）。

9.2.2.9.2 测试过程

下列测试过程适用于安全加固：
a） 检测基于 Android 开发的移动应用是否采用了防逆向、防篡改的安全措施，措施是否生效；
b） 检测基于 iOS 开发的移动应用是否采用了防逆向、防篡改的安全措施，措施是否生效。

9.2.2.9.3 测试结果

安全加固测试结果，应满足下列要求：
a） 基于 Android 开发的移动应用应进行防逆向、防篡改安全措施的保护，且措施生效；
b） 基于 iOS 开发的移动应用应进行防逆向、防篡改安全措施的保护，且措施生效。

9.2.2.10 运行环境安全

9.2.2.10.1 测试项

运行环境安全的测试项中 a）、b）项适用于 Android 版，同时 a）项适用于 iOS 版，具体如下：
a） 移动应用应对运行环境进行安全检测，限制移动应用在超级用户权限下使用（中风险）；
b） 基于 Android 开发的移动应用应限制在模拟器环境下运行（低风险）。

9.2.2.10.2 测试过程

运行环境安全的测试过程中 a）、b）项适用于 Android 版，同时 a）项适用于 iOS 版，具体如下：
a） 检测移动应用是否可在超级用户权限下使用；
b） 检测基于 Android 开发的移动应用是否可在模拟器环境下运行。

9.2.2.10.3 测试结果

运行环境安全的测试结果中 a）、b）项适用于 Android 版，同时 a）项适用于 iOS 版，具体如下：
a） 移动应用应在运行前对运行环境进行安全检测，不可在超级用户权限下使用；
b） 基于 Android 开发的移动应用应不可在模拟器环境下运行。

9.2.2.11 算法安全

9.2.2.11.1 测试项

算法安全的测试项同时适用于 Android 版和 iOS 版。移动应用应采用国家管理部门认可的加解密算法，如 SM2、SM3、SM4 算法等（中风险）。

9.2.2.11.2 测试过程

检测移动应用对隐私数据进行存储或传输时是否使用了加密算法，使用了哪种加密算法。

9.2.2.11.3 测试结果

移动应用应采用国家管理部门认可的加解密算法，如 SM2、SM3、SM4 算法等对隐私数据进行存储或传输。

9.2.2.12 权限安全

9.2.2.12.1 测试项

权限安全的测试项仅适用于 Android 版。基于 Android 开发的移动应用应确保权限最小化，移动应用申请的权限应与功能相对应，避免冗余权限的滥用（中风险）。

9.2.2.12.2 测试过程

检测移动应用安装时启用了哪些权限，是否存在移动应用功能不需要的权限。

9.2.2.12.3 测试结果

移动应用启用的权限应与功能相对应，不存在多余权限。

9.2.2.13 防调试

9.2.2.13.1 测试项

由于 iOS 类移动应用的封装性、发布渠道等具备一定的安全性，且移动应用在发布前 iOS 商店会进行安全性审核，防调试测试项不适用于 iOS 类移动应用，仅适用于 Android 版，具体如下：

a） 基于 Android 开发的移动应用不应开启调试功能（中风险）；
b） 基于 Android 开发的移动应用应不可输出调试日志（中风险）；
c） 基于 Android 开发的移动应用应具备防动态调试功能（低风险）。

9.2.2.13.2 测试过程

下列测试过程适用于防调试：

a） 检测移动应用是否开启调试功能；
b） 检测移动应用是否调用调试日志函数；
c） 尝试对移动应用进行动态调试。

9.2.2.13.3 测试结果

防调试测试结果，应满足下列要求：

a） 移动应用应关闭调试功能；
b） 移动应用应无调试日志输出；
c） 移动应用应可防止动态调试攻击。

9.2.2.14 防非法备份

9.2.2.14.1 测试项

由于 iOS 类移动应用的封装性、发布渠道等具备一定的安全性，且移动应用在发布前 iOS 商店会进行安全性审核，防非法备份测试项不适用于 iOS 类移动应用，仅适用于 Android 版。基于 Android 开发的移动应用应可防止应用数据被非法备份（高风险）。

9.2.2.14.2 测试过程

检测移动应用是否开启了允许备份功能。

9.2.2.14.3 测试结果

移动应用不应开启允许备份功能，防止数据被非法备份。

9.2.2.15 防病毒

9.2.2.15.1 测试项

防病毒的测试项仅适用于 Android 版，基于 Android 开发的移动应用应不包含病毒文件（高风险）。

9.2.2.15.2 测试过程

检测移动应用是否包含病毒。

9.2.2.15.3 测试结果

移动应用应不包含病毒文件。

9.2.2.16 通道安全

9.2.2.16.1 测试项

通道安全的测试项同时适用于 Android 版和 iOS 版，具体如下：

a） 移动应用与服务器进行通信时应对通信数据进行加密保护（高风险）；

b） 移动应用与服务器进行通信时应对通信数据进行数据完整性校验（中风险）。

9.2.2.16.2 测试过程

下列测试过程适用于通道安全：

a） 检测移动应用与服务器通信过程中数据是否为明文；

b） 尝试修改移动应用与服务器的通信数据并发送给服务器。

9.2.2.16.3 测试结果

通道安全测试结果，应满足下列要求：

a） 移动应用与服务器通信时应对通信数据进行加密保护；

b） 移动应用与服务器通信时采用校验码技术或密码技术保证隐私数据在传输过程中的完整性。

9.2.3 渗透测试

9.2.3.1 测试项

渗透测试的测试项同时适用于 Android 版和 iOS 版，移动应用应不存在越权访问、SQL 注入攻击、跨站脚本攻击、会话重放攻击、明文传输、敏感信息泄露、文件上传漏洞等已知安全漏洞（高风险）。

9.2.3.2 测试过程

检查是否存在越权访问漏洞、明文传输漏洞、SQL 注入漏洞、XSS 跨站脚本漏洞、文件上传漏

洞、后台地址泄露漏洞、敏感信息泄露漏洞、命令执行漏洞、目录遍历漏洞、会话重放攻击漏洞、跨站请求伪造漏洞、任意文件包含漏洞、任意文件下载漏洞、设计缺陷错误、设计逻辑错误、XML 实体注入漏洞、开放高危端口和无关端口、登录功能验证码漏洞、不安全的 Cookies 漏洞、SSL3.0 漏洞、SSRF 漏洞、默认口令/弱口令、不安全的 http 请求方法等已知安全漏洞（测试方法示例参见附录 B）。

9.2.3.3 测试结果

未发现明显可利用的安全漏洞。

附 录 A
（资料性附录）
黑 盒 测 试 方 法

A.1 功能分解

功能分解是将需求规格说明中每一个功能加以分解，确保各个功能被全面测试。功能抽象中程序被看成一种抽象的功能层次，每个层次可标识被测试的功能。层次结构中的某一功能由其下一层功能定义。按照功能层次进行分解，可以得到众多的最低层次的子功能，以这些子功能为对象，进行测试用例设计。数据抽象中，数据结构可以由抽象数据类型的层次图来描述，每个抽象数据类型有其取值集合。程序的每一个输入和输出量的取值集合用数据抽象来描述。

功能分析是一种较常用的方法，步骤如下：

a） 使用程序设计中的功能抽象方法把程序分解为功能单元；

b） 使用数据抽象方法产生测试每个功能单元的数据。

A.2 等价类划分

等价类划分是在分析需求规格说明的基础上，把程序的输入域划分成若干部分，然后在每部分中选取代表性数据形成测试用例，步骤如下：

a） 划分有效等价类：对规格说明有意义、合理的输入数据所构成的集合；

b） 划分无效等价类：对规格说明无意义、不合理的输入数据所构成的集合；

c） 为每一个等价类定义一个唯一的编号；

d） 为每一个等价类设计一组测试用例，确保覆盖相应的等价类。

A.3 边界值划分

边界值分析是针对边界值进行测试的。对满足边界值的输入可以发现计算差错，对不满足的输入可以发现域差错。此方法会为其他测试方法补充一些测试用例，绝大多数测试都会用到此方法。使用等于、小于或大于边界值的数据对程序进行测试的方法就是边界值分析方法，步骤如下：

a） 通过分析规格说明，找出所有可能的边界条件；

b） 对每一个边界条件，给出满足和不满足边界值的输入数据；

c） 设计相应的测试用例。

A.4 判定表

判定表由四部分组成：条件桩、条件条目、动作桩、动作条目。任何一个条件组合的取值及其相应要执行的操作构成规则，条目中的每一列是一条规则。条件引用输入的等价类，动作引用被测软件的主要功能处理部分，规则就是测试用例。建立并优化判定表，把判定表中每一列表示的情况写成测试用例。该方法的使用有以下要求：

a） 规格说明以判定表形式给出，或很容易转换成判定表；

b） 条件的排列顺序不会影响执行哪些操作；

c） 规则的排列顺序不会影响执行哪些操作；

d） 每当某一规则的条件已经满足，并确定要执行的操作后，不必检验其他规则；

e） 如果某一规则的条件得到满足，将执行多个操作，这些操作的执行与顺序无关。

A.5 因果图

因果图方法是通过画因果图，把自然语言描述的功能说明转换为判定表，然后为判定表的每一列设计一个测试用例。如果需求规格说明中含有输入条件的组合，宜采用本方法。有些软件的因果图可能非常庞大，以至于根据因果图得到的测试用例数目非常大，此时不宜使用本方法。步骤如下：

a） 分析程序规格说明，引出原因（输入条件）和结果（输出结果），并给每个原因和结果赋予一个标识符；

b） 分析程序规格说明中语义的内容，并将其表示成连接各个原因和各个结果的“因果图”；

c） 在因果图上标明约束条件；

d） 通过跟踪因果图中的状态条件，把因果图转换成有限项的判定表；

e） 把判定表中每一列表示的情况生成测试用例。

A.6 随机测试

随机测试指测试输入数据是在所有可能输入值中随机选取的。测试人员只需规定输入变量的取值区间，在需要时提供必要的变换机制，使产生的随机数服从预期的概率分布。该方法获得预期输出比较困难，多用于可靠性测试和系统强度测试。

A.7 猜错法

猜错法是有经验的测试人员，通过列出可能有的差错和易错情况表，写出测试用例的方法。

A.8 正交实验法

正交实验法是从大量的实验点中挑出适量的、有代表性的点，应用正交表，合理地安排实验的一种科学的实验设计方法。利用正交实验法来设计测试用例时，首先要根据被测软件的规格说明书找出影响功能实现的操作对象和外部因素，把它们当作因子，而把各个因子的取值当作状态，生成二元的因素分析表。然后，利用正交表进行各因子的状态组合，构成有效的测试输入数据集，并由此建立因果图。这样得出的测试用例的数目将大大减少。

附 录 B
（资料性附录）
渗透测试方法示例

B.1 渗透测试

渗透测试方法示例见表 B.1。

表 B.1 渗透测试方法示例

序号	测试项	测试方法示例
1	越权访问漏洞	首先使用工具抓取 A 用户功能链接，然后登录 B 用户对此链接进行访问； 通过抓包工具抓取 A 用户 ID 并将此 ID 改成 B 用户的 ID，查看是否可以操作 B 用户的功能或查看 B 用户的数据； 通过抓包工具替换不同用户 cookie 的方法进行测试
2	明文传输	使用工具抓取有关用户口令的数据包（登录、添加用户、更改密码等），查看数据包中提交的相关参数； 系统内所涉及的口令等隐私数据传输地方应做加密处理； 不应使用 MD5 等易被破解的加密方式和 Base64 编码、URL 编码等方式解决此类问题
3	SQL 注入漏洞	在系统请求参数后加上 SQL 测试语句如“and 1=1”，即地址栏中填入“http://www.example.com/page.xxx?name=value and 1=1”，返回正确； 在被测参数后加上测试语句“and 1=2”，返回错误，则说明存在 SQL 注入漏洞； 若请求参数为字符型参数则使用“' and '1'='1”，“' and '1'='2”。 如确定存在 SQL 注入漏洞，则需要手工构造 SQL 注入语句或者使用 Sqlmap 进一步测试
4	XSS 漏洞	如在输入参数中输入<script>alert（123）</script>等 XSS 测试语句，如 http://example.com/index.php?user=<script>alert（123）</script>，若弹出提示框，则说明存在跨站漏洞
5	上传漏洞	如果客户端脚本限制了上传文件的类型（例如允许 GIF 文件），则上传一个后缀名为 gif 的木马文件如 hacker.gif，然后配置 http proxy（Burp Suite）进行 http 请求拦截； 重新点击“浏览”按钮，并选择 hacker.gif，确认上传； 在 Burp Suite 拦截的 http 请求数据中，将 hacker.gif 修改为 hacker.jsp，再发送请求数据；查找文件上传的路径，构造访问链接，在浏览器地址栏输入构造链接如：http://www.example.com/hacker.jsp，访问该后门程序，取得 webshell，也可通过文件解析漏洞和截断等测试该漏洞
6	后台泄露漏洞	根据抓取系统 URL 构造出一些常见的 Web 服务器后台泄露 URL 地址如： Tomcat 控制台 URL：http://www.example.com:8080/manager/html Weblogic 控制台 URL：http://www.example.com:7001/console
7	敏感信息泄露	查看前端 JS 文件或者通过 Burp Suite 输入异常测试字符（如：“’”“-”等），显示以下信息都属于敏感信息泄露： 1）网站绝对路径； 2）SQL 语句； 3）中间件版本； 4）程序异常等
8	命令执行	已知某页面 URL（假设为 http://www.example.com/abc.jsp）接收参数，且参数中接收类似于系统命令的字符（假设为 cmd=ls）； 则更改参数的值为其他命令，可以尝试以下一些字符串：Net user、Ipconfig、cat /etc/ passwd，并在浏览器地址栏输入更改后的 URL，如 http://www.example.com/abc. jsp? cmd=ipconfig，命令可以被执行； 使用 Weblogic、Struts2 专用的漏洞检测工具，检测中间件框架漏洞（包括 Struts2 S2-016、S2-019、S2-037、S2-045、Weblogic、JBoss 漏洞等）

表 B.1（续）

序号	测试项	测试方法示例
9	目录遍历漏洞	在浏览器地址栏输入网站目录，如 http://www.example.com/test/，查看 test 文件夹内的文件能否被列出来
10	关键会话重放攻击	使用工具抓取网站登录会话请求包； 使用用户或密码字典替代登录请求会话中对应的用户或密码参数，开始尝试暴力破解，如发现响应码和响应长度不同，则此条会话中猜解的用户名和密码正确或用户名正确
11	CSRF（跨站请求伪造）	登录网站，使用工具构造 CSRF POC，并保存在 HTML 文件中； 如访问 HTML 文件成功，则构造 HTML 的预期功能实现，并确认存在 CSRF 漏洞
12	任意文件包含/任意文件下载	已知某页面 URL，如 http://www.example.com/viewfile.do?filename=report.xls，更改其参数的值为其他文件路径； 并在浏览器地址栏中尝试以下更改参数后的 URL： http://www.example.com/viewfile.do?filename=../etc/passwd http://www.example.com/viewfile.do?filename=../../etc/passwd http://www.example.com/viewfile.do?filename=../../../etc/passwd 观察能否获得/etc/passwd 文件内容
13	设计缺陷/逻辑错误	在测试中可以根据下列方法进行测试： 首先，测试人员应尽量理解业务系统。 其次，提炼各种业务场景和工作流程。 最后，设计业务逻辑测试。测试时可按照以下方法： 1）修改数值（如构造 SQL 语句可被执行）； 2）验证码爆破（如 4 位数字验证码可暴力破解）； 3）修改响应包（如通过修改登录响应包，密码错误时可登录系统）； 4）修改密码（如修改密码逻辑问题）； 5）服务端无有效验证； 6）未授权访问（如 URL 连接未授权访问，Redis 未授权访问漏洞，Memcache 未授权访问漏洞）； 7）返回密码信息（如响应包中返回密码信息）； 8）密码明文存储（如前台存储明文密码信息）； 9）登录用户提示（如提示用户是否存在，可猜解正确的用户名）等
14	XML 实体注入	使用 Burp Suite 抓包，查找请求会话中带有 XML 格式的请求，然后对 XML 文件进行操作，如在<?xml version="1.0" encoding="ISO-8859-1"?>后插入如下内容： Linux 系统： <?xml version="1.0" encoding="UTF-8"?> <!DOCTYPE UserInfo [<!ENTITY name SYSTEM"file:///etc/passwd">] > <UserInfo> <name>&name; </name> </UserInfo> Window 系统： <?xml version="1.0" encoding="UTF-8"?> <!DOCTYPE UserInfo [<!ENTITY name SYSTEM"file:///c:/boot.ini">] > <UserInfo> <name>&name; </name> </UserInfo> 如果可读取服务器上的文件内容，则存在该漏洞
15	检测存在风险的无关服务和端口	使用端口扫描工具查看系统所在检测环境的端口开放情况，对系统内端口情况以及漏洞进行检测，分析检测环境是否开放了高危端口和无关端口。高危端口应关闭或提供安全防护措施，无关端口应关闭。高危端口不限于 135、139 端口如：

表 B.1（续）

序号	测试项	测试方法示例
15	检测存在风险的无关服务和端口	445 端口 CVE-2008-4250 Microsoft Windows Server 服务 RPC 请求缓冲区溢出漏洞（MS08-067） CVE-2017-0143 到 CVE-2017-0148 Microsoft Windows SMB Server 远程代码执行漏洞（MS17-010）
16	登录功能验证码漏洞	使用工具抓取网站登录请求数据包； 在带有验证码功能的登录数据包中，可以进行会话重放攻击或者通过更改请求数据包中参数使验证码功能不生效或关闭同样可以达到会话重放攻击的目的
17	不安全的 Cookies	在使用工具拦截的请求数据中，查看用户 Cookies 中的信息，如显示用户名或密码等敏感信息，则为不安全的 Cookies
18	SSL 漏洞	主要针对 OpenSSL 心脏出血漏洞，漏洞编号 CVE-2014-0160，使用检测脚本对该漏洞进行检测
19	SSRF 漏洞	对被检系统进行检测，如果该系统网络内存在 192.168.1.22IP 地址，则在浏览器内访问以下链接：http://www.example.com/uddiexplorer/SearchPublicRegistries.jsp?operator=http://192.168.1.22&rdoSearch=name&txtSearchname=sdf&txtSearchkey=&txtSearchfor=&selfor=Business+location&btnSubmit=Search，通过更改 IP 后，例如将链接中 IP 更改为“192.168.1.23”（系统中不存在的 IP），如果更改 IP 前后服务器响应状态不同，则存在该漏洞
20	默认口令/弱口令	人工查看默认口令/弱口令包括： 1）应用程序弱口令； 2）中间件程序弱口令等
21	其他漏洞	其他不常见漏洞，如不安全的 http 请求方法等

附 录 C
（资料性附录）
综 合 评 价 方 法

C.1 功能测试、非功能测试评价方法

C.1.1 单项判定方法

单一质量特性评价标准、测试问题级别定义如下：

a） 测试用例覆盖需求率达到 100%；

b） 测试用例回归执行率达到 100%；

c） 测试后移动应用没有出现致命性问题（ZM）和严重性（YZ）问题；

d） 不影响移动应用正常使用的一般性问题（YB）、建议性问题（JY）的数量少于 3 个。

问题严重等级说明见表 C.1。

表 C.1 问题严重等级说明

I	致命问题	是指移动应用崩溃、数据丢失、数据毁坏或停止提供服务等导致移动应用无法再继续运行的问题	必须修改
II	严重问题	主要功能实现错误或遗漏、骨干流程不可用，核心功能违反软件规范、业务规范等导致移动应用无法实现正常功能的问题	必须修改
III	一般问题	非主要功能错误，移动应用的 UI 布局不合理及罕见的不影响主要业务操作等问题	不影响移动应用正常使用的一般性问题、建议性问题的数量少于 3 个
IV	建议问题	软件实际操作与使用说明不符，软件功能不方便使用，不符合用户普遍操作习惯等问题	

C.1.2 整体评价方法

对测试结果进行综合考查，参测移动应用的“功能测试、效率（性能）、兼容性、易用性、可维护性、可移植性、可靠性、用户文档集要求”8 大质量特性结果均为“通过”且满足单一判定结果的移动应用，在测试报告中确定为“通过”；对任意一项单一质量特性不通过的移动应用，在测试报告中确定为“不通过”。

C.2 安全评价方法

C.2.1 单项判定方法

C.2.1.1 安全功能测试判定方法

移动应用客户端的安全功能检测项判定方法如下：

a） 测试项中仅有一项测试结果的，如满足测试结果，则判定为该项符合，如不满足测试结果，则判定为不符合；

b） 测试项中有多项测试结果的，如全部满足测试结果，则判定为该项符合，如不满足全部测试结果，则判定为不符合，如只满足部分测试结果，则判定为部分符合；

c） 如果某测试项，在特定移动应用软件系统中不适用，则可判定该测试项为“不适用”，不影响

整体测试结论。

C.2.1.2 渗透测试测试判定方法

移动应用客户端的渗透测试检测项判定方法：测试项中未发现明显可利用安全漏洞，则渗透测试整体结论为“未发现明显可利用安全漏洞”。

C.2.2 整体评价方法

评价方法描述测试人员执行完测试方法过程，产生各种测试证据后，如何依据这些测试证据来判定移动应用软件系统是否满足安全性要求。安全检测报告应给出移动应用软件系统安全测试结论，确认移动应用软件系统达到相应安全要求的程度。测试结论评价如下：

a） 安全功能所有测试项均为“符合”，且渗透测试结果为“未发现明显可利用安全漏洞”，则安全测试整体结论为“符合”；

b） 安全功能所有高风险或中风险的测试项均为“符合”，低风险的测试项中存在不多于 3 项“部分符合”或“不符合”，且渗透测试结果为“未发现明显可利用安全漏洞”，则安全测试整体结论为“符合”；

c） 安全功能高风险或中风险的测试项中存在“部分符合”或“不符合”，或安全功能低风险的测试项中存在超过 3 项“部分符合”或“不符合”，或渗透测试结果为“存在明显可利用安全漏洞”，则安全测试整体结论为“不符合”。

附 录 D
（资料性附录）
测 试 工 具

D.1 功能测试工具

D.1.1 测试管理工具

测试管理工具对测试需求、测试计划、测试用例、测试实施进行管理，并且测试管理工具还包括对缺陷的跟踪管理。测试管理工具能让测试人员、开发人员或相关人员通过一个中央数据仓库，在不同地方就能交互信息。

D.1.2 自动化测试工具

通过录制、检测和回放用户的应用操作，将被测系统的输出记录同预先给定的标准结果比较，自动化测试工具能够有效地帮助测试人员对移动应用软件的不同发布版本的功能进行测试，提高测试人员的工作效率和质量。其主要目的是检测应用程序是否能够达到预期的功能并正常运行。

D.2 非功能测试工具

D.2.1 服务端性能测试工具

服务端性能测试工具的主要目的是度量移动应用软件的可扩展性和性能，是一种预测系统行为和性能的自动化测试工具。在实施并发负载过程中，通过实时性能监测来确认和查找问题，并针对所发现问题对系统性能进行优化，确保应用的成功部署。性能测试工具能够对整个移动应用软件服务端进行测试，通过这些测试，企业能最大限度地缩短测试时间，优化性能，保证移动应用上线后的平稳运行。

D.2.2 客户端性能测试工具

客户端性能测试工具的主要目的是评估移动应用软件在终端运行时的性能、可靠性和兼容性。在测实施测试过程中，通过自动化手段将移动应用软件客户端分发至各移动终端，针对特定的场景或遍历整个移动应用页面，实时监测试客户端占用移动终端的资源情况及运行时的兼容适配性。客户端运行在大批量的移动终端上时，可有效降低人工操作成本，提高测试效率和准确性。

D.3 安全测试工具

D.3.1 安全功能测试工具

安全功能测试多以人工查看加以辅助工具判断安全功能正确性及存在的风险，安全功能测试涉及工具较多，工具目的主要以达到测试需求，满足测试目标为基础。

D.3.2 渗透测试工具

通常的黑客攻击包括预攻击、攻击和后攻击三个阶段。预攻击阶段主要指一些信息收集和漏洞扫描的过程；攻击过程主要是利用第一阶段发现的漏洞或弱口令等脆弱性进行入侵；后攻击是指在获得攻击目标的一定权限后，对权限的提升、后面安装和痕迹清除等后续工作。与黑客的攻击相比，渗透

测试仅仅进行预攻击阶段的工作，并不对系统本身造成危害，即仅仅通过一些信息搜集手段来探查系统的弱口令、漏洞等脆弱性信息。为了进行渗透测试，通常需要一些专业工具进行信息收集。渗透测试工具种类繁多，涉及广泛，按照功能和攻击目标分为网络扫描工具、通用漏洞检测、应用漏洞检测三类。

D.3.2.1 网络扫描工具

网络扫描工具其目的在于发现目标的操作系统类型、开放端口等基本信息，为后续的扫描工作做基础。事实上，利用操作系统本身的一些命令如 ping、telnet、nslookup等也可以对目标的信息进行判断，但是利用专业的工具可以给出更加全面和准确的判断。

D.3.2.2 通用漏洞检测工具

在获取了目标主机的操作系统、开放端口等基本信息后，通常利用通用漏洞扫描工具检测目标系统所存在的漏洞和弱口令。通用漏洞主要指操作系统本身或者安装的应用软件所存在的漏洞，通常是指缓冲区漏洞，例如 MS-08-067、oracle 的漏洞。由于系统开启了 135、139、445、1433、1521 等应用程序端口，同时没有及时安装补丁，使得外来主机可以通过相应的端口发送恶意的请求从而获取不应当获得的系统权限。通常漏洞检测工具应具备程序扫描与漏洞库，漏洞库应及时更新，符合相关电力移动应用安全要求。

D.3.3 代码安全工具

代码安全工具其目的在于发现源代码中存在的一些语义缺陷、安全漏洞等，应用静态源代码安全扫描的主要价值在于能够快速、准确地查找、定位和修复软代码中存在的安全风险，增加工具投资所带来的最大效益，节约代码安全分析的成本，最终开发出安全的、可靠的移动应用软件。

D.4 测试辅助工具

这些工具本身并不执行测试，例如它们可以生成测试数据，抓取客户端与服务器通信时的数据包等，为测试提供数据准备和结果判断依据。