ICS 35.240.01
L70

团　　体　　标　　准

T/ISC 0018—2022

移动互联网应用程序（App）数据安全测评能力要求

Data security test and evaluation capability requirements for mobile Internet applications

2022 - 11 - 01 发布　　2023 - 02 - 01 实施

中　国　互　联　网　协　会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国互联网协会归口。

本标准主要起草单位：中国信息通信研究院、中国电子技术标准化研究院、中国软件评测中心、国家工业信息安全发展研究中心、深圳市网安计算机安全检测技术有限公司、北京智游网安科技有限公司（爱加密）、北京梆梆安全科技有限公司、成都思维世纪科技有限责任公司

本标准主要起草人：解伯延、王丹辉、谢玮、魏薇、陈湉、刘行、高超、唐刚、秦晓磊、余宇舟、张渊、秦博阳、钟子呈、黄伟杰、韩云、章明珠、姜会安、任江辉、曾礼、方宁、卢佐华

移动互联网应用程序（App）数据安全测评能力要求

1 范围

本文件提供了了移动互联网应用程序数据安全测评工作的指南，对移动互联网应用程序数据安全测评工作要求、测评内容进行了描述和规范，并针对移动互联网应用程序源文件、存储、交互、安全防护等方面的数据安全风险给出相应测评方法。

本标准适用于移动互联网应用程序数据安全测评，可供测评机构开展移动互联网应用程序数据安全测评工作时作为参考，为相关机构强化测评能力、健全技术手段提供指引，也可供应用程序开发者、运营者在实施数据安全防护策略时参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 37988—2019 信息安全技术 数据安全能力成熟度模型

3 术语和定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1 移动互联网应用程序 mobile internet application

运行在移动智能终端上的应用程序。

注：包括移动智能终端预置、下载安装的应用程序和小程序。

3.1.2 数据安全 data security

数据安全，是指通过采取必要措施，保障数据得到有效保护和合法利用，并持续处于安全状态的能力。

[来源：GB/T 37988—2019，定义 3.1]

3.1.3 识别 identification

涉及查找、辨识和记录潜在数字证据的过程。

[来源：ISO/IEC 27037:2012，定义 3.12]

3.2 缩略语

下列缩略语适用于本文件。

App 移动互联网应用程序 mobile internet application

4 移动互联网应用程序数据安全测评能力模型

App数据安全测评能力管理要求明确测评对象、测评启动条件、测评实施流程以及测评报告规范，App数据安全测评能力技术要求分为基础级与增强级，测评内容主要包括与数据安全明确相关的风险、漏洞等测评项，测评能力模型如图1所示。

基础级App数据安全测评技术要求覆盖数据存储机制、传输情况、权限调用行为等易于识别、核验的测评项。

增强级App数据安全测评技术要求覆盖恶意攻击防范、数据安全机制等需要一定技术能力储备及人工核验的较为复杂的测评项。

图 1　App数据安全测评能力模型

5　移动互联网应用程序数据安全测评能力管理要求

5.1　测评对象要求

App数据安全测评的对象是App运营者、分发服务平台等App业务相关方开发、运营或分发的App软件产品。

5.2　测评启动条件要求

除行业主管部门组织开展的数据安全测评工作以外，满足下列情形之一的，App运营者、应用分发平台及时启动测评，测评可自行进行或委托第三方进行：

a）App于应用分发平台上线或于产品官网等其他渠道提供下载时开展测评；

b）根据App运营者、应用分发平台自身计划开展测评，如定期测评，以及在App业务功能、程序逻辑等发生较大变化时开展测评；

c）行业主管部门要求开展数据安全测评时开展测评；

d）国家法律法规有相关要求或满足国家法律法规有关情形时开展测评。

5.3 测评实施流程要求

测评实施流程包括如下三个阶段：

a）准备阶段

测评准备阶段包括制定测评方案、确定测评小组人员、获取被测App样本、明确测评项目范围、评估测评环境及测评工具。

b）实施阶段

测评实施阶段包括采用工具扫描、沙箱模拟、动态测试、人工干预、功能遍历等方式，发现App数据安全风险，评估App数据安全保护能力，针对风险制定整改措施。

c）结束阶段

测评结束阶段包括对实施过程、测评结果、整改方案等进行审查核验，根据准备阶段制定的测评报告模板编制测评报告。

5.4 测评报告规范要求

测评报告应当包括以下组成部分（参见附录E）：

a）App基本信息，包括被测App样本名称、版本、系统类型、样本来源、样本获取时间、样本文件大小、样本文件MD5、运营者名称等；

b）测评设备信息，包括测评设备软硬件名称、软硬件配置、版本等；

c）测评项目说明，包括测评覆盖的风险项类别、名称、简要说明等；

d）测评结果汇总，包括测评发现风险数量统计、风险分布统计、风险名称、描述、对应整改建议等；

e）测评结果明细，详细记录测评过程中发现的风险所在的文件路径、字段,对风险所在位置进行截图存证并详细标注,同时针对发现的数据安全风险提出针对性的整改、修复建议。

6 移动互联网应用程序数据安全测评能力技术要求

6.1 基础级 App 数据安全测评能力技术要求

6.1.1 源文件安全

基础级数据源文件安全问题测评以App源代码、资源文件、安全配置风险为核心，应对App源文件中Java代码反编译、核心文件或关键明文字符串加密保护措施、测试代码残留、注入漏洞等进行测评。

重点测评项目包括但不限于Js资源文件未加密、So文件破解、单元测试配置风险、WebSQL注入漏洞、Plists信息泄漏、明文字符串泄露、外部函数显式调用风险、代码未混淆等（参见附录A、附录B）。

6.1.2 数据存储安全

基础级数据存储安全问题测评以App功能配置、重要信息存储为核心，应对Webview组件保存用户、密码功能的设置、安全策略有效性、本地存储数字证书文件的安全性、加密算法的密钥设置、明文存储情况等进行测评。

重点测评项目包括但不限于Webview明文存储密码、Webview File同源策略绕过、明文数字证书、调试日志函数调用、应用数据任意备份、密钥硬编码、数据库明文存储、配置文件信息明文存储等（参见附录A、附录B）。

6.1.3 数据交互安全

基础级数据交互安全问题测评以App组件配置、传输机制为核心，应对组件注册方式、组件导出属性设置、数据传输协议情况等进行测评。

重点测评项目包括但不限于动态注册Receiver、Activity组件导出、Service组件导出、Broadcast Receiver组件导出、Content Provider组件导出、HTTP传输数据风险、缺乏有效的Token机制等（参见附录A、附录B）。

6.1.4 数据安全防护机制

基础级App数据安全防护机制测评以安全防护机制脆弱性为核心，应对Webview组件证书校验情况、输入数据监听或按键位置记录、界面截图或录制、Webview组件接口函数调用策略、SD卡后动态加载行为等进行测评。

重点测评项目包括但不限于Webview绕过证书校验、输入监听、截屏攻击、Webview远程代码执行、从Sdcard加载So风险、主键截屏漏洞等（参见附录A、附录B）。

6.2 增强级 App 数据安全测评能力技术要求

6.2.1 源文件安全

增强级源文件安全问题测评在基础级测评的基础上，以源文件合法性、完整性保障机制为核心，应对App签名证书验证机制、App签名算法安全性、App源文件篡改、二次打包防护情况、调试证书使用情况等进行测评。

重点测评项目包括但不限于应用签名未校验、应用签名算法不安全、篡改/二次打包风险、使用调试证书发布应用、注入攻击、Webview组件跨域访问风险等（参见附录C、附录D）。

6.2.2 数据存储安全

增强级数据存储安全问题测评在基础级测评的基础上，以本地数据存储安全防护机制、组件安全配置为核心，应对C层代码动态调试情况、组件读写权限设置、数据全局可读写状态等进行测评。

重点测评项目包括但不限于动态调试攻击、数据库注入、Shared Preferences数据全局可读写、Internal Storage数据全局可读写、GetDir数据全局可读写等（参见附录C、附录D）。

6.2.3 数据交互安全

增强级数据交互安全问题测评在基础级测评的基础上，以App数据交互组件配置安全、加密传输协议有效性为核心，应对组件之间数据交互机制、违法Intent请求或异常数据防护策略、证书安全校验机制等进行测评。

重点测评项目包括但不限于Intent组件隐式调用、Intent Scheme URL攻击、HTTPS未校验服务器证书等（参见附录C、附录D）。

6.2.4 数据安全防护机制

增强级数据安全问题防护机制测评在基础级测评的基础上，以App面临的数据安全威胁、安全防护机制脆弱性为核心，应对界面劫持防护机制、绕过用户验证运行、动态注入防护策略、执行命令过滤检验等进行测评。

重点测评项目包括但不限于界面劫持、“应用克隆”漏洞、Root设备运行、动态注入攻击、Janus签名漏洞、XcodeGhost、ZipperDown等（参见附录C、附录D）。

附 录 A
（资料性附录）
基础级 Android App 数据安全重点测评项目及方法

A.1 源文件安全

1）Js 资源文件未加密

编号	基础级-源文件-Android-01
测评项目	Js 资源文件未加密
问题描述	APK 的 Js 文件中可能包含重要显示界面以及 Js 执行代码，如果 Js 文件被读取可能导致功能逻辑泄露，如果被篡改，可能被植入钓鱼页面或者恶意代码，造成用户的敏感信息泄露。
测评方法	解析 Js 资源文件，校验资源文件是否经加密保护。

2）So 文件破解

编号	基础级-源文件-Android-02
测评项目	So文件破解
问题描述	So 文件被破解可能导致核心功能的汇编代码甚至源代码泄露，暴露客户端的核心功能逻辑，攻击者可以利用这些信息窃取客户端的敏感数据，包括手机号、密码；截获与服务器之间的通信数据；绕过业务安全认证流程，直接篡改用户账号信息；对服务器接口发起攻击等。
测评方法	检测 So 文件是否经加密保护，被测 App 企业应对自身 So 文件风险进行修复。

3）单元测试配置

编号	基础级-源文件-Android-03
测评项目	单元测试配置风险
问题描述	测试代码存在配置单元中，和配置单元进行关联的风险。应用 Androidmanifest.xml 文件保留有单元测试配置项或者源码中保留有单元测试代码，容易导致客户端功能暴露，可能导致泄露客户端关键业务逻辑。
测评方法	反编译 APK 文件，检测配置单元中是否存在测试代码。

4）WebSQL 注入

编号	基础级-源文件-Android-04
测评项目	WebSQL 注入漏洞
问题描述	HTML5 可以在浏览器里面存数据库。攻击者通过 SQL 注入点进行 WebSQL 攻击，可能导致存储的敏感数据信息被查询泄露，例如账户名，密码等。
测评方法	反编译 APK 文件，检测 App 是否使用 HTML5 数据库，其配置是否存在 WebSQL 注入漏洞。

A.2 数据存储安全

1）Webview 明文存储密码

编号	基础级-数据存储-Android-01

测评项目	Webview 明文存储密码风险
问题描述	Android 的 Webview 组件中默认打开了提示用户是否保存密码的功能，可能明文存储用户密码等信息并导致相关信息泄露。
测评方法	反编译 APK 文件，检测 Webview 组件的密码保存属性值是否允许保存密码。

2）Webview File 同源策略绕过

编号	基础级-数据存储-Android-02
测评项目	Webview File 同源策略绕过漏洞
问题描述	应用程序一旦使用 WebView，同时支持 File 域，并打开了对 JavaScript 的支持，就能利用 JavaScript 的延时执行，绕过 File 协议的同源检查，并能够访问应用程序的私有文件，导致敏感信息泄露。
测评方法	反编译 APK 文件，检测代码 Webview 组件的全局文件访问属性值是否运行同源策略绕过。

3）明文数字证书

编号	基础级-数据存储-Android-03
测评项目	明文数字证书风险
问题描述	APK 内明文存储的数字证书如果被篡改，客户端可能连接到假冒的服务端上，导致用户名、密码等信息被窃取；如果明文证书被盗取，可能造成传输数据被截获解密，用户信息泄露，或者伪造客户端向服务器发送请求，篡改服务器中的用户数据或造成服务器响应异常。
测评方法	通过解压 APK 文件包，获取签名证书文件，校验证书文件的内容是否存在明文字符。

4）调试日志函数调用

编号	基础级-数据存储-Android-04
测评项目	调试日志函数调用风险
问题描述	调试日志函数可能输出重要的日志文件，其中包含的信息可能导致客户端用户信息泄露，暴露客户端代码逻辑等。
测评方法	反编译 APK 文件，监测是否存在允许 Log 日志输出和关键异常信息打印相关代码，如是，则查验 Log 是否含有配置信息、代码逻辑等内容。

5）应用数据任意备份

编号	基础级-数据存储-Android-05
测评项目	应用数据任意备份风险
问题描述	Android 2.1 以上的系统可为 App 提供应用程序数据的备份和恢复功能，当相关属性没有显式设置为 False 时，攻击者可对 App 的应用数据进行备份和恢复，从而可能获取明文存储的用户敏感信息，如用户的密码、证件号、手机号、交易密码、身份令牌、服务器通信记录等。利用此类信息攻击者可伪造用户身份，盗取用户账户资产，或者直接对服务器发起攻击。
测评方法	反编译 APK 文件，检测 AndroidManifest 文件的允许备份属性值。

6）密钥硬编码

编号	基础级-数据存储-Android-06
测评项目	密钥硬编码漏洞
问题描述	密钥硬编码是指在代码中直接将加密算法的密钥设置为一个固定值，通过反编译可以直接查看密钥内容，整个加密算法将形同虚设。密钥硬编码，可直接造成加密数据被破解，客户端与服务器之间的通信内容被破解，导致应用内的加密文件被破解，或是用户的敏感信息泄露。
测评方法	反编译 APK 文件，检测代码中是否存在常量密钥。

A.3 数据交互安全

1）动态注册 Receiver

编号	基础级-数据交互-Android-01
测评项目	动态注册 Receiver
问题描述	BroadcastReceiver 组件的动态注册易被忽略默认可导出，如果没有指定权限访问控制，可以被任意外部应用访问，向其传递 Intent 来执行特定的功能。因此，动态注册的 BroadcastReceive 可能导致拒绝服务攻击、应用数据泄漏或是越权调用等风险。
测评方法	反编译 APK 文件，检测 BroadcastReceiver 组件注册方式是否是动态注册。

2）Activity 组件导出

编号	基础级-数据交互-Android-02
测评项目	Activity 组件导出
问题描述	Activity 作为组成 Apk 的四个组件之一，是 Android 程序与用户交互的界面，如果 Activity 打开了导出权限，可能被系统或者第三方的 App 直接调出并使用。Activity 导出可能导致登录界面被绕过、拒绝服务攻击、程序界面被第三方恶意调用等风险。
测评方法	反编译 APK 文件，检测 Activity 组件导出属性值设置和 Intent-filter 是否配置 Action。

3）Service 组件导出

编号	基础级-数据交互-Android-03
测评项目	Service组件导出
问题描述	Service 作为组成 Apk 的四个组件之一，一般作为后台运行的服务进程，如果设置了导出权限，可能被系统或者第三方的 App 直接调出并使用。Service 导出可能导致拒绝服务攻击，程序功能被第三方恶意调用等风险。
测评方法	通过工具提取应用的 Android Manifest 文件并解析，获取所有注册的 Service 组件，检测属性值设置和 Intent-filter 是否配置 Action。

4）Broadcast Receiver 组件导出

编号	基础级-数据交互-Android-04
测评项目	Broadcast Receiver组件导出
问题描述	Broadcast Receiver 作为组成 Apk 的四个组件之一，对外部事件进行过滤接收，并根据消息内容执行响应，如果设置了导出权限，可能被系统或者第三方的 App 直接调出并使用。Broadcast Receiver 导出可能导致敏感信息泄露、

	登录界面被绕过等风险。
测评方法	通过工具提取应用的 Android Manifest 文件并解析，获取所有注册的 Receiver 组件，检测属性值设置和 Intent-filter 是否配置 Action。

5）Content Provider 组件导出

编号	基础级-数据交互-Android-05
测评项目	Content Provider组件导出
问题描述	Content Provider 组成 APK 的四个组件之一，是应用程序之间共享数据的容器，可以将应用程序的指定数据集提供给第三方的 App，如果设置了导出权限，可能被系统或者第三方的 App 直接调出并使用。Content Provider 导出可能导致程序内部的敏感信息泄露，数据库 SQL 注入等风险。
测评方法	通过 APKTool 提取应用的 Android Manifest 文件并解析，获取所有注册的 Provider 组件，检测属性值设置和 Intent-filter 是否配置 Action。

6）HTTP 传输数据

编号	基础级-数据交互-Android-06
测评项目	HTTP 传输数据风险
问题描述	使用 HTTP 协议进行数据传输，未对数据传输进行加密，可导致数据包遭截获、传输内容泄露。
测评方法	检测 App 是否使用 HTTP 协议传数数据，且数据是否包含敏感信息。

7）缺乏有效的 Token 机制

编号	基础级-数据交互-Android-07
测评项目	缺乏有效的 Token 机制
问题描述	如果被测应用没有使用有效的 Token 机制，可对登陆响应中的服务器返回的鉴权信息进行修改，即可绕过服务器鉴权，直接访问系统内部信息。
测评方法	拦截应用对用户登陆的响应信息，检测是否能对登陆响应中的服务器返回的 token 鉴权信息进行修改。

A.4 数据安全防护机制

1）Webview 绕过证书校验

编号	基础级-数据防护-Android-01
测评项目	Webview绕过证书校验
问题描述	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并忽略，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”。
测评方法	反编译 APK 文件，检测证书校验过程中是否存在忽略证书错误的情况。

2）输入监听

编号	基础级-数据防护-Android-02
测评项目	输入监听
问题描述	应用程序中的敏感信息通常主要来源于使用者的直接输入，如果用户的输入数据被监听或者按键位置被记录，很可能导致用户的输入数据被获取。

	Android 系统的默认输入键盘中通常都面临数据监听的风险。
测评方法	反编译 APK 文件，检测 Activity 中是否存在对系统软键盘的监听隐藏。

3）截屏攻击

编号	基础级-数据防护-Android-03
测评项目	截屏攻击
问题描述	截屏攻击是指对 App 应用运行中的界面进行截图或者录制。截屏攻击的主要对象是 Android 应用中的身份认证、登录界面和资金操作界面。在 Android5.0 中新增了屏幕录制接口，无需特殊权限即可实现屏幕录制，并且攻击程序可以通过自定义的字符覆盖掉系统的录屏提示，诱导用户在不知情的情况下启动屏幕录制功能。
测评方法	反编译 APK 文件，检测是否调用了防止个人敏感信息输入或展示的界面被截图和录制的方法。

4）Webview 远程代码执行

编号	基础级-数据防护-Android-04
测评项目	Webview远程代码执行
问题描述	Webview 是 Android 用于浏览网页的组件，其包含的接口函数 AddJavascriptInterface 可以将 Java 类或方法导出以供 JavaScript 调用，实现网页 JS 与本地 JAVA 的交互。可能导致被篡改的 URL 中存在的恶意代码被执行，用户手机被安装木马程序，甚至手机被远程控制。
测评方法	反编译 APK 文件，检测代码 Webview 加载网页是否调用接口函数 AddJavascriptInterface

5）从 Sdcard 加载 So 文件

编号	基础级-数据防护-Android-05
测评项目	从 Sdcard 加载 So 风险
问题描述	出于节省 APK 包大小，或者动态升级 So 文件的原因，App 程序可能将部分 So 文件存储或者下载于 Sdcard 上，然后进行动态加载。
测评方法	检测 App 是否允许 So 文件存储或者下载于 Sdcard 后动态加载。

附 录 B
（资料性附录）
基础级 iOS App 数据安全重点测评项目及方法

B.1 源文件安全

1）Plists 信息泄漏

编号	基础级-源文件-iOS-01
测评项目	Plists 信息泄漏
问题描述	Plist 文件通常用于储存用户设置，也可以用于存储捆绑的信息。此类文件可能存在信息泄露风险。
测评方法	解压 IPA 文件目录，检测其 plist 文件是否包含敏感信息。

2）明文字符串泄露

编号	基础级-源文件-iOS-02
测评项目	明文字符串泄露
问题描述	程序中常常包含明文字符串信息，如果不做加密保护，很容易通过字符串泄露使用的关键算法、密码等信息，需要评估明文字符串是否包含敏感或关键的信息，建议进行加密保护。
测评方法	反编译 IPA 文件，检测 App 代码文件中是否存在明文的敏感或关键信息。

3）外部函数显示调用

编号	基础级-源文件-iOS-03
测评项目	外部函数显示调用风险
问题描述	攻击者通过静态分析程序中存在的显式外部函数调用，很容易获取和跟踪程序逻辑，然后对外部函数调用进行 Hook 拦截，甚至进行篡改业务逻辑等恶意行为。
测评方法	反编译 IPA 文件，检测代码中是否存在显式调用外部函数的情况。

4）代码未混淆

编号	基础级-源文件-iOS-04
测评项目	代码未混淆
问题描述	iOS 代码未混淆则代码内方法名、变量名、类名、包名等这些元素可读,无法对源代码实现逻辑分支混淆和控制流平坦化从而隐藏关键逻辑，可能导致敏感安全信息被窃取。
测评方法	反编译 IPA 文件，获取 App 代码结构信息（如类名、函数列表）、函数名称等，检测内容是否可读。

B.2 数据存储安全

1）密钥硬编码

编号	基础级-数据存储-iOS-01
测评项目	密钥硬编码漏洞
问题描述	密钥硬编码是指在代码中直接将加密算法的密钥设置为一个固定值，通过反

	编译可以直接查看密钥内容，整个加密算法将形同虚设。密钥硬编码，可直接造成加密数据被破解，客户端与服务器之间的通信内容被破解，导致应用内的加密文件被破解，或是用户的敏感信息泄露。
测评方法	反编译 IPA 文件，检测代码中是否存在常量密钥。

2）数据库明文存储

编号	基础级-数据存储-iOS-02
测评项目	数据库明文存储风险
问题描述	iOS 自带的 SQLite 数据库没有内置的加密支持。如果 App 未对数据进行加密后再存储，那么 App 会直接以明文格式将包含敏感信息的数据存储在 SQLite 数据库中。一旦该数据库中的数据被直接查询、备份，或者数据恢复，存储在 SQLite 中未加密的敏感信息将会直接暴露。
测评方法	反编译 IPA 文件，检测 SQLite 数据库中，是否存在明文存储的用户敏感信息，如账户名，密码，后台连接地址，服务器等相关信息。

3）配置文件信息明文存储

编号	基础级-数据存储-iOS-03
测评项目	配置文件信息明文存储风险
问题描述	iOS 应用包中的属性列表文件 Plist 文件主要用于存储用户设置及 App 的配置信息，包括用户名、密码或其它个人敏感信息，直接以明文存储敏感信息易被获取。
测评方法	反编译 IPA 文件，检测是否对 Plist 文件使用系统加密库。

B.3 数据交互安全

1）HTTP 传输数据

编号	基础级-数据交互-iOS-01
测评项目	HTTP 传输数据风险
问题描述	使用 HTTP 协议进行数据传输，未对数据传输进行加密，可导致数据包遭截获、传输内容泄露。
测评方法	检测 App 是否使用 HTTP 协议传数数据，且数据是否包含敏感信息。

2）缺乏有效的 Token 机制

编号	基础级-数据交互-iOS-02
测评项目	缺乏有效的 Token 机制
问题描述	如果被测应用没有使用有效的 Token 机制，可对登陆响应中的服务器返回的鉴权信息进行修改，即可绕过服务器鉴权，直接访问系统内部信息。
测评方法	拦截 App 用户登陆的响应数据包，检测是否能对登陆响应中的服务器返回的 token 鉴权信息进行修改。

B.4 数据安全防护机制

1）主键截屏

编号	增强级-数据防护-iOS-01

测评项目	主键截屏漏洞
问题描述	iOS 系统在程序退出的时候，会保存程序当前的快照，如果退出的时候页面含有密码等关键信息未进行处理则存在安全隐患。
测评方法	打开 App 的任意含敏感信息的界面后，检测 App 是否允许保存含有敏感信息的截图。

附 录 C
（资料性附录）
增强级 Android App 数据安全测评项目及方法

C.1 源文件安全

1）应用签名未校验

编号	增强级-源文件-Android-01
测评项目	应用签名未校验
问题描述	未使用签名证书的 App，可导致 App 被仿冒盗版，甚至可能被添加钓鱼代码、病毒代码、恶意代码，导致用户敏感信息泄露。
测评方法	对 APK 进行重新签名，检测是否可以成功安装并启动成功。

2）应用签名算法不安全

编号	增强级-源文件-Android-02
测评项目	应用签名算法不安全
问题描述	使用陈旧的 SHA-1 哈希算法，可能导致签名遭破解。
测评方法	反编译 APK 文件，检测代码是否含有 SHA-1 签名算法。

3）篡改/二次打包

编号	增强级-源文件-Android-03
测评项目	篡改打包风险
问题描述	缺少安装包完整性、可靠性验证机制，可导致遭恶意修改、篡改、二次打包 App 被安装运行，危害开发者版权和经济利益，并导致用户遭到恶意功能、代码侵害。
测评方法	反编译 APK 文件，重新打包安装该篡改应用，检测是否存在篡改后二次打包风险。

4）使用调试证书发布应用

编号	增强级-源文件-Android-04
测评项目	使用调试证书发布应用
问题描述	使用调试证书发布应用可能导致 App 无法在应用市场上架，以及 App 应用无法成功升级的情况。另外，证书的不一致性可能造成 App 使用的签名校验措施频繁改动或者被迫取消，存在应用被二次打包风险。
测评方法	获取 App 签名证书文件并通过工具获取证书所有者信息，判断是否为调试证书。

C.2 数据存储安全

1）动态调试攻击

编号	增强级-数据存储-Android-01
测评项目	动态调试攻击
问题描述	C 层代码动态调试风险可能导致不法分子利用 GDB、IDA、Ptrace 等调试器跟踪运行目标程序，查看、修改内存中的代码和数据，甚至分析篡改程序的业

	务逻辑，对客户关键数据或者服务器进行恶意攻击。
测评方法	安装并运行 App，检测目标进程是否可动态调试。

2）数据库注入

编号	增强级-数据存储-Android-02
测评项目	数据库注入
问题描述	由于 Content Provider 组件读写权限设置不当，并且未对 Sql 查询语句的字段参数作过滤判断，App 本地数据库可能被注入攻击。
测评方法	反编译 APK 文件，扫描 Content Provider URL，并执行其中的查询，检测是否有异常返回。

3）Shared Preferences 数据全局可读写

编号	增强级-数据存储-Android-03
测评项目	Shared Preferences 数据全局可读写
问题描述	Shared Preferences 是 Android 系统的本地数据存储方式之一，如果配置不恰当模式或属性值时，可能导致储存于 Shared Preferences 文件中的敏感信息被其他程序读写。
测评方法	反编译 APK 文件，检测 Shared Preferences 数据是否全局可读写。

4）Internal Storage 数据全局可读写

编号	增强级-数据存储-Android-04
测评项目	Internal Storage 数据全局可读写
问题描述	Internal Storage 作是 Android 系统的本地数据存储方式之一，如果配置不恰当模式或属性值时，可能导致储存于 Internal Storage 文件中的敏感信息被其他程序读写。
测评方法	反编译 APK 文件，检测 Internal Storage 数据是否全局可读写。

5）GetDir 数据全局可读写

编号	增强级-数据存储-Android-05
测评项目	GetDir 数据全局可读写
问题描述	Context.GetDir 是访问 Android 系统的 Internal Storage 的一个重要方式。如果配置不恰当模式或属性值时，可能导致储存于该文件夹中的敏感信息被其他程序读写。
测评方法	反编译 APK 文件，检测 GetDir 数据是否全局可读写.

C.3 数据交互安全

1）Intent 组件隐式调用

编号	增强级-数据交互-Android-01
测评项目	Intent 组件隐式调用
问题描述	Intent 通常用于 Activity、Service、Broadcast Receiver 等组件之间进行信息传递，可能存在该信息被未知的第三方应用劫持的风险。
测评方法	检测 Smali 代码通过 Intent 启动组件时是否进行了显式调用。

2）Intent Scheme URL 攻击

编号	增强级-数据交互-Android-02
测评项目	Intent Scheme URL攻击
问题描述	利用 Intent Scheme URLs 可以通过 Web 页面发送 Intent 来启动 App 应用。攻击者可构造特殊格式的 URL 直接向系统发送意图，启动 App 应用的 Activity 组件或者发送异常数据，导致应用的敏感信息泄露或者应用崩溃。
测评方法	检测使用 Intent.ParseUrl 解析时，是否对来源组件进行安全校验。

3）HTTPS 未校验服务器证书

编号	增强级-数据交互-Android-03
测评项目	HTTPS未校验服务器证书
问题描述	使用 HTTPS 协议时，客户端必须对服务器证书进行完整校验，以验证服务器是真实合法的目标服务器。如果没有校验，客户端可能与仿冒的服务器建立通信链接，即“中间人攻击”。
测评方法	反编译 APK 文件，检测 HTTPS 在验证服务器证书时，是否对服务器证书进行安全校验。

C.4 数据安全防护机制

1）界面劫持

编号	增强级-数据防护-Android-01
测评项目	界面劫持
问题描述	界面劫持是指当客户端程序调用一个应用界面时，被恶意的第三方程序探知，如果该界面组件是恶意程序预设的攻击对象，恶意程序立即启动自己的仿冒界面并覆盖在客户端程序界面之上,用户可能在无察觉的情况下将敏感信息输入到仿冒的信息输入界面中，恶意程序再把这些数据返回到服务器中，完成钓鱼攻击。
测评方法	启动木马程序对目标应用进行界面覆盖，检测 App 是否弹出明显的提示或终端进程。

2）应用克隆

编号	增强级-数据防护-Android-02
测评项目	“应用克隆”漏洞
问题描述	当 Android 应用中存在包含 Webview 的可被导出 Activity 组件时，若该 WebView 允许通过 File Url 对 Http 域进行访问，并且未对访问的路径进行严格校验，则可能导致“应用克隆”漏洞攻击。
测评方法	反编译 APK 文件，检测通过 File Url 对 Http 域进行访问时，是否对访问路径进行严格校验。

3）Root 设备运行

编号	增强级-数据防护-Android-03
测评项目	Root设备运行
问题描述	获取 Android 的 Root 权限通常是通过系统漏洞,替换或添加可绕过用户验证

	的可执行 SU 程序，Root 权限环境下运行可能导致 App 私有目录遭访问、传输遭劫持等风险
测评方法	Root 环境下安装 App，检测其是否可正常运行，是否具备防 Roor 运行机制。

4）动态注入攻击

编号	增强级-数据防护-Android-04
测评项目	动态注入攻击
问题描述	通过操作系统特定机制,可利用系统 API 将代码写入到目标进程并让其执行，进而实施 Hook，监控程序运行、获取敏感信息等。
测评方法	安装 App 后，检测是否可利用系统 API 成功进行动态注入。

5）Janus 签名

编号	增强级-数据防护-Android-05
测评项目	Janus 签名漏洞
问题描述	Janus 签名漏洞允许攻击者绕过安卓系统的 Signature Scheme V1 签名机制，进而使用篡改过的 App 安装获取原始 App 的所有数据，直接进行篡改。（影响 Android4.0-Android7.0 版本）
测评方法	检测 App 是否支持 Android7.0 以下系统运行，如是，则反编译后检测代码是否使用 V1+V2 混合签名模式。

附 录 D
（资料性附录）
增强级 iOS App 数据安全测评项目及方法

D.1 源文件安全

1）篡改/二次打包

编号	增强级-源文件-iOS-01
测评项目	篡改/二次打包风险
问题描述	缺少安装包完整性、可靠性验证机制，可导致遭恶意修改、篡改、二次打包 App 被安装运行，危害开发者版权和经济利益，并导致用户遭到恶意功能、代码侵害。
测评方法	反编译 IPA 文件，篡改 App 代码、资源文件内容后重新打包，检测篡改后 IPA 包是否可正常安装、运行。

2）注入攻击

编号	增强级-源文件-iOS-02
测评项目	注入攻击风险
问题描述	通过注入攻击将恶意代码写入目标进程，可能加载其它可执行程序，进而实施 Hook，监控程序运行、获取敏感信息。
测评方法	修改代码中的环境变量相关值，并插入动态库检测是否成功执行。

3）Webview 组件跨域访问

编号	增强级-源文件-iOS-03
测评项目	Webview组件跨域访问风险
问题描述	iOS 平台应用若未对访问的路径进行严格校验，攻击者可利用 Webview 组件漏洞，远程获取手机应用沙盒内所有本地文件系统内容，包括浏览器的 Cookies、用户的配置文件、文档等敏感信息，甚至远程打开并加载恶意 HTML 文件等。
测评方法	反编译 IPA 文件，检测 App 是否含有 Webview 组件跨域访问风险代码。

D.2 数据安全防护机制

1）界面劫持

编号	增强级-数据防护-iOS-01
测评项目	界面劫持
问题描述	界面劫持是指当客户端程序调用一个应用界面时，被恶意的第三方程序探知，如果该界面组件是恶意程序预设的攻击对象，恶意程序立即启动自己的仿冒界面并覆盖在客户端程序界面之上,用户可能在无察觉的情况下将敏感信息输入到仿冒的信息输入界面中，恶意程序再把这些数据返回到服务器中，完成钓鱼攻击。
测评方法	启动木马程序对目标应用进行界面覆盖，检测 App 是否弹出明显的提示或终端进程。

2）XcodeGhost

编号	增强级-数据防护-iOS-02
测评项目	XcodeGhost
问题描述	iOS 应用的开发者如果使用非苹果公司官方渠道下载的 Xcode 工具开发应用程序可能被非正版开发工具植入恶意代码。
测评方法	反编译 IPA 文件，搜索 Xcode 漏洞的关键字“init.icloud - analysis.com”，检测 App 是否含有相关代码。

3）ZipperDown

编号	增强级-数据防护-iOS-03
测评项目	ZipperDown
问题描述	iOS 平台 App 调用第三方库实现解压的功能时，可能出现目录穿越漏洞导致 App Container 目录下的任意文件覆盖，造成应用崩溃或恶意代码执行。
测评方法	反编译 IPA 文件，定位解压函数位置，检测 App 下载路径相关代码是否存在 ZipperDown 漏洞。

附 录 E
（资料性附录）
App 数据安全测评报告模板

（App 名称）数据安全测评报告

编号 ：单位名称缩写-App 名称缩写-测试日期-测试序号（例:XTY-XXX-20210101-0001）

App 名称：...

App 版本：...

App 运营者：...

（测评单位名称）

年 月 日

一、 App 基本信息

项目	描述
App 名称\版本	
系统类型	
样本来源	
样本获取时间	
样本文件大小	
样本文件 MD5	
运营者名称	

二、 测评设备信息

序号	软硬件名称	软硬件配置/版本

三、 测评项目说明

序号	类别	测评项	说明

四、 测评结果汇总

本次测评共发现..个风险，主要包括...（风险名称）。

序号	风险名称	问题描述	整改建议

五、 测评结果明细

（一）...(安全风险类别)

1.1 ...(安全风险名称)

【测评结果】：...（是否存在风险）

【问题描述】：...（安全问题描述、风险判断依据描述）

【风险截图】：...（提供风险所在文件路径、字段证据截图,并对风险所在字段进行标注）

【整改建议】：...（针对发现的安全风险、漏洞提出针对性的整改、修复建议。）