ICS 33.030
CCS M21

团 体 标 准

T/CCSA 549—2024 T/CAAAD 002-2024

互联网广告 自动化工具安全测评规范

Internet advertising——Security testing specification for automation tools

2024－07－03 发布 2024－10－03 实施

中国广告协会 中国通信标准化协会 发 布

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专利的责任。

本文件由中国广告协会和中国通信标准化协会共同提出，并分别归口。

本标准起草单位：中国信息通信研究院、中国广告协会、深圳市腾讯计算机系统有限公司、北京奇虎科技有限公司、华为软件技术有限公司、北京快手科技有限公司、北京风行在线技术有限公司、秒针信息技术有限公司、北京国双科技有限公司、尼洱市场研究（上海）有限公司、央视市场研究股份有限公司、北京回旋加速网络科技有限公司。

本标准主要起草人：陈婉莹、杨正军、杨阳、潘柳琴、刘骁、霍焰、崔妍、李光、倪萍、李克鹏、姚一楠、欧阳书馨、落红卫、赵笑凤、刘力泉、吴充、葛宝勤、苏婧、王弢。

引　言

为适应信息通信发展对标准文件的需求，由中国通信标准化协会和中国广告协会共同组织制定本文件，推荐有关方面采用。有关对本文件的建议和意见，向中国通信标准化协会和中国广告协会反映。

近年来，随着移动智能终端设备的普及、移动互联网累计接入流量的增长以及移动互联网用户的增加，互联网营销也在随之由PC端向移动端迁移，形成移动互联网广告新模式。在移动互联网广告领域，包括广告展示、移动归因、广告监测、营销分析等等多种类型的服务均可通过以SDK为主要模式的第三方自动化工具包来完成，但第三方自动化工具包仍存在不少问题。第三方自动化工具包开发往往侧重于功能性的完善，而在安全性方面投入较少，且由于第三方自动化工具包被广泛使用到大量的App中，造成漏洞的影响范围非常大。同时，部分第三方自动化工具包存在隐瞒收集用户个人信息的行为，间接造成App违规，甚至被直接下架。明明是第三方自动化工具包的问题，最终买单的却是广大用户和App开发者。

为解决行业痛点问题，提升第三方自动化工具包安全性，帮助App开发者评估第三方自动化工具包安全，有必要制定针对互联网广告第三方自动化工具包的安全测评规范。

互联网广告 自动化工具安全测评规范

1　范围

本文件规定了对互联网广告自动化工具恶意行为、代码安全、自身安全、算法安全、网络通讯安全、数据交互安全、数据存储安全、组件安全、漏洞与风险防范、与APP联动、隐私协议等方面的测评要求与方法。

本文件适用于对第三方移动互联网广告自动化工具的安全测评，可包括程序、脚本、接口、软件开发工具包（SDK）等多种形式，也可为移动互联网广告自动化工具设计开发提供参考。

2　规范性引用文件

本文件没有规范性引用文件。

3　术语、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

移动互联网广告自动化工具　mobile internet advertising automation tools

为实现移动互联网广告展示、归因、监测、分析等相关功能开发的，面向应用软件提供的代码打包文件，可包括程序、脚本、接口、软件开发工具包（SDK）等。

3.2　缩略语

下列缩略语适用于本文件。

AES：高级加密标准（Advanced Encryption Standard）
API：应用程序接口（Application Programming Interface）
APP：应用软件（Application）
ARC：自动引用计数（Automatic Refrence Counting）
DES：数据加密标准（Data Encryption Standard）
ECB：电码本（Electronic Codebook）
HTTP：超文本传输协议（Hyper Text Transfer Protocol）
HTTPS：超文本传输安全协议（Hyper Text Transfer Protocol over SecureSocket Layer）
OFB：输出反馈（Output-Feedback）
PIE：执行地址无关（Position Independent Executable）
SD：安全数字（Secure Digital）
SDK：软件开发工具包 （Software Development Kit）
SSP：栈溢出保护功能（Stack Smashing Protection）
TDES：三重数据加密标准（Triple Data Encryption Standard）
URL：统一资源定位系统（Uniform Resource Locator）
VPN：虚拟专用网络（Virtual Private Network）

4　概述

4.1　测评方法

移动互联网广告自动化工具的安全测评规范中涉及的方法主要包括：

——文档审核:文档审核是指被测评机构向测评机构提供包含有测评产品相关信息的说明文档，以向测评员提供产品安全策略、澄清风险或提供证据；
——自动化测评：自动化测评指使用自动化测评工具，对测评产品进行漏洞扫描、静态测试等，分析测评产品的代码安全；
——使用验证：使用验证指测评机构对集成到 APP 中的测评产品进行使用、分析，以验证测评产品的自动化测评结果，以及验证是否存在有不符合提交文档的情况。

4.2　结果描述

本文件描述了移动互联网广告自动化工具安全测评规范。测评结果有以下两种：
——未见异常：通过测评方法没有发现存在违反安全测评要求的情况，符合安全要求；
——存在风险：通过评估方法发现存在违反安全测评要求的情况，存在一定风险，风险分为高危、中危、低危三等。

4.3　测评流程

测评流程如图1所示。

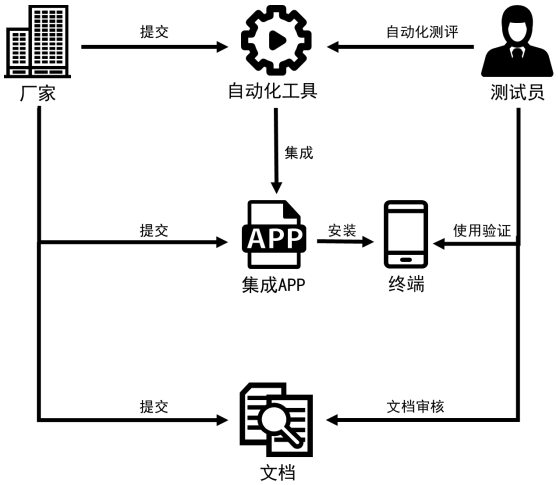

图 1　评估流程

被评估机构向评估机构提供相关产品以及说明文档，产品包括：
——测评产品；
——集成测评产品的 APP；
——功能说明；
——技术文档；
——用户手册。
文档包括：
——隐私协议；
——合作合同；
——安全保证性文档；
——其他证明文档。
测评机构测试、验证被测评机构提供的产品、文档，得出测评结果。

4.4　测评内容

移动互联网广告自动化工具的安全测评内容框架如图2所示，其中Android端和iOS端不同格式文件安全测评详细测试项参见附录A，与APP联动测评和隐私协议测评文档审核记录表模版参见附件B。

图 2　测评内容框架

5　Android 端安全测评要求与方法

5.1　恶意行为检测

5.1.1　敏感内容

5.1.1.1　敏感函数检测

测评项目	敏感函数检测
风险等级	中危
测评要求	应避免在代码中调用获取个人信息的敏感行为函数，如为必要调用应在“隐私协议”中告知。
测评方法	文档审核+自动化测评+使用验证
预期结果	1、自动化测评未在代码中检测出敏感行为函数的实际调用行为； 2、自动化测评在代码中检测出敏感行为函数的实际调用行为，但已在“隐私协议”中告知且为功能必要调用。
备注	以上预期结果满足一条即认定为安全。

5.1.1.2　敏感词汇检测

测评项目	敏感词汇检测
风险等级	中危
测评要求	代码中不应含有黄赌毒、暴力、宗教、政治、人权等敏感词汇。
测评方法	自动化测评
预期结果	不存在敏感词汇。
备注	无

5.2　安全规范检测

5.2.1　源代码安全

5.2.1.1　SO 文件加固检测

测评项目	SO 文件加固检测
风险等级	高危
测评要求	SO 文件应通过加固保护具备防反编译、防调试能力。
测评方法	自动化测评
预期结果	SO 文件已做加固保护，具备防反编译、防调试能力。
备注	无

5.2.1.2　Java 代码混淆检测

测评项目	Java 代码混淆检测
风险等级	低危
测评要求	Java 代码应进行混淆。
测评方法	自动化测评
预期结果	Java 代码已混淆。
备注	在需要给外部进行 API 的调用的情况下，保留了部分类和函数名称，没有全部进行混淆可以认定为安全。

5.2.1.3　日志函数泄漏风险

测评项目	日志函数泄漏风险
风险等级	高危
测评要求	应在正式版本中关闭调试日志，或者确保日志的输出使用了正确的级别，涉及敏感数据的日志信息在发布版本中被关闭。
测评方法	自动化测评+使用验证
预期结果	1、自动化测评未检测出调试日志函数的调用； 2、自动化测评检测出调试日志函数的调用，但为必要日志且不涉及敏感数据。
备注	以上预期结果满足一条即认定为安全。

5.2.1.4　动态加载 SO 文件风险

测评项目	动态加载 SO 文件风险
风险等级	低危
测评要求	不应动态加载 SO 文件，如将 SO 文件存储或者下载到 sdcard 中，先将 SO 文件拷贝到应用私有目录下非 lib 文件夹中，然后使用 System.load 函数进行加载。
测评方法	自动化测评
预期结果	不存在动态加载 SO 文件。
备注	无

5.2.1.5　测试信息残留风险

测评项目	测试信息残留风险
风险等级	低危
测评要求	正式版本不应携带的测试信息，如内部服务器地址等。
测评方法	自动化测评
预期结果	不存在测试信息残留。
备注	无

5.2.1.6　URL 硬编码检测

测评项目	URL 硬编码检测
风险等级	低危
测评要求	代码中不应存在非必要的 URL 硬编码，如必须存在 URL 不应指向非公开地址。
测评方法	自动化测评
预期结果	1、不存在 URL 硬编码； 2、存在 URL 硬编码，但是必须且指向公开地址。
备注	以上预期结果满足一条即认定为安全。

5.2.1.7　内网测试信息残留风险

测评项目	内网测试信息残留风险

风险等级	低危
测评要求	代码中不应包含内网测试信息。
测评方法	自动化测评
预期结果	不存在残留内网测试信息。
备注	无

5.2.1.8　启动隐藏服务风险

测评项目	启动隐藏服务风险
风险等级	中危
测评要求	不应存在隐藏程序启动 Activity。
测评方法	自动化测评
预期结果	不存在启动隐藏服务。
备注	无

5.2.1.9　动态加载 DEX 文件风险

测评项目	动态加载 DEX 文件风险
风险等级	低危
测评要求	不应存在动态加载 DEX 文件，如在代码中使用 DexClassLoader 或 PathClassLoader 动态加载 dex 文件、apk 文件、jar 文件。
测评方法	自动化测评
预期结果	不存在动态加载 dex 文件。
备注	必须动态加载的场景，需要对于 DEX 文件进行签名或 MD5 校验。

5.2.1.10　硬编码风险

测评项目	硬编码风险
风险等级	高危
测评要求	代码中不应存放的固定值数据，包括密钥硬编码风险、残留账号密码信息、残留手机号码信息、残留 Email 信息。
测评方法	自动化测评
预期结果	不存在硬编码。
备注	无

5.2.1.11　单元测试配置风险

测评项目	单元测试配置风险
风险等级	低危
测评要求	代码中不应保留有单元测试代码或 AndroidManifest.xml 文件不应保留有单元测试配置项。
测评方法	自动化测评
预期结果	代码和 AndroidManifest.xml 文件不存在单元测试配置。
备注	无

5.2.2　自身安全

5.2.2.1　资源文件泄露风险

测评项目	资源文件泄露风险
风险等级	中危
测评要求	如 JavaScript 脚本等可能包含资源文件中的重要显示界面及执行，应进行保护处理，如 Assets 目录加密
测评方法	自动化测评
预期结果	不存在未做保护的资源文件。

备注	无

5.2.2.2　证书明文存储风险

测评项目	证书明文存储风险
风险等级	高危
测评要求	数字证书不应明文存储。
测评方法	自动化测评
预期结果	不存在证书明文存储。
备注	无

5.2.2.3　Java 层动态调试风险

测评项目	Java 层动态调试风险
风险等级	低危
测评要求	AndroidManifest.xml 文件中的调试标记应关闭。
测评方法	自动化测评
预期结果	不存在 Java 层动态调试。
备注	无

5.2.2.4　应用测试模式发布风险

测评项目	应用测试模式发布风险
风险等级	低危
测评要求	AndroidManifest.xml 文件中不应设置 TestOnly 模式。
测评方法	自动化测评
预期结果	不存在应用测试模式发布。
备注	无

5.2.2.5　资源文件包含 APK 检测

测评项目	资源文件包含 APK 检测
风险等级	低危
测评要求	资源文件不应包含 APK 文件。
测评方法	自动化测评
预期结果	资源文件不包含 APK。
备注	无

5.2.2.6　开发商自定义服务风险

测评项目	开发商自定义服务风险
风险等级	低危
测评要求	不应存在开发商自定义的未进行权限控制的 Service 组件。
测评方法	自动化测评
预期结果	不存在开发商自定义服务。
备注	无

5.2.2.7　未保护的自定义权限风险

测评项目	未保护的自定义权限风险
风险等级	低危
测评要求	自定义权限的保护等级(android:protectionLevel 属性)不应设置为 normal，或没有显示设置(默认情况也为 normal)。
测评方法	自动化测评
预期结果	不存在未保护的自定义权限。

备注	无

5.2.3　算法使用安全

5.2.3.1　AES/DES/TDES 加密算法不安全使用风险

测评项目	AES/DES/TDES 加密算法不安全使用风险
风险等级	高危
测评要求	AES/DES/TDES 算法工作模式不应使用 ECB 或 OFB。
测评方法	自动化测评
预期结果	不存在 AES/DES/TDES 加密算法不安全使用。
备注	无

5.2.3.2　RSA 加密算法不安全使用风险

测评项目	RSA 加密算法不安全使用风险
风险等级	高危
测评要求	RSA 算法密码长度应设置大于 1024 位长度，且使用过程中宜使用相对安全的工作模式以及填充方式。
测评方法	自动化测评
预期结果	不存在 RSA 加密算法不安全使用。
备注	无

5.2.4　网络通讯安全

5.2.4.1　HTTPS 未校验服务器证书风险

测评项目	HTTPS 未校验服务器证书风险
风险等级	中危
测评要求	应使用默认的 HTTPS 证书验证机制，不应使用使用重写的 X509TrustManager 类，重写的 X509TrustManager 类，其中的 checkServerTrusted()方法不对验证失败做任何处理，即不对证书进行正确校验结果。
测评方法	自动化测评
预期结果	不存在 HTTPS 未校验服务器证书风险。
备注	无

5.2.4.2　HTTPS 未校验主机名风险

测评项目	HTTPS 未校验主机名风险
风险等级	中危
测评要求	应使用默认的 HTTPS 证书验证机制，不应使用 X509TrustManager 类检查证书是否合法并且是否未过期或使用 HostnameVerifier 类检查证书中的主机名与使用该证书的服务器的主机名是否一致，重写的 HostnameVerifier，其中的 Verify()方法不对主机名验证失败做任何处理，即不对主机名进行正确校验。
测评方法	自动化测评
预期结果	不存在 HTTPS 未校验主机名风险。
备注	无

5.2.4.3　HTTPS 允许任意主机名风险

测评项目	HTTPS 允许任意主机名风险
风险等级	中危
测评要求	Android 允许开发者重定义证书的验证方法，调用的

	setHostnameVerifier 方法不应被配置为接受任何服务器主机名（ALLOW_ALL_HOSTNAME_VERIFIER）或者配置为空。
测评方法	自动化测评
预期结果	不存在 HTTPS 允许任意主机名风险。
备注	无

5.2.4.4　传输通道风险

测评项目	HTTP 传输通道风险
风险等级	高危
测评要求	不应直接使用 HTTP 协议登录账户或交换数据。
测评方法	自动化测评
预期结果	不存在 HTTP 传输通道。
备注	无

5.2.4.5　中间人攻击风险

测评项目	中间人攻击风险
风险等级	高危
测评要求	应对服务器端证书做校验，且不应该包含服务器证书的私钥信息或其他 pkcs 文件。
测评方法	自动化测评
预期结果	不存在中间人攻击风险
备注	无

5.2.4.6　访问境外服务器风险

测评项目	访问境外服务器风险
风险等级	高危
测评要求	不应访问境外服务器。
测评方法	自动化测评
预期结果	不存在访问境外服务器。
备注	无

5.2.4.7　联网环境检测

测评项目	联网环境检测
风险等级	低危
测评要求	不应使用网络代理服务。
测评方法	自动化测评
预期结果	不存在设置代理服务。
备注	无

5.2.5　数据交互安全

5.2.5.1　getDir 数据全局可读写风险

测评项目	getDir 数据全局可读写风险
风险等级	中危
测评要求	如使用 Context.getDir（String name , int mode）函数，第二个参数不应使用 MODE_WORLD_READABLE 或 MODE_WORLD_WRITEABLE 模式或不应在 AndroidManifest 中设置 android:sharedUserId。
测评方法	自动化测评
预期结果	该应用不存在 getDir 数据全局可读写风险
备注	无

5.2.5.2　Intent 敏感数据泄露风险

测评项目	Intent 敏感数据泄露风险
风险等级	低危
测评要求	如果目标 Activity 与源 Activity 在不同的 Task 中，不应将 Intent 用于 Activity 之间的数据传递。
测评方法	自动化测评
预期结果	不存在 Intent 敏感数据泄露。
备注	无

5.2.5.3　PendingIntent 误用 Intent 风险

测评项目	PendingIntent 误用 Intent 风险
风险等级	中危
测评要求	PendingIntent 不应创建 Intent 给其他应用，并且允许这个应用以与自己相同的权限来执行这个 Intent。
测评方法	自动化测评
预期结果	不存在 PendingIntent 误用 Intent。
备注	无

5.2.5.4　发送广播信息泄漏风险

测评项目	发送广播信息泄漏风险
风险等级	低危
测评要求	不应使用 sendStickyBroadcast 函数。
测评方法	自动化测评
预期结果	不存在发送广播信息风险。
备注	无

5.2.5.5　随机数不安全使用风险

测评项目	随机数不安全使用风险
风险等级	低危
测评要求	SecureRandom 类不应使用 setSeed 方法，应使用/dev/urandom 或者/dev/random 来初始化伪随机数生成器。
测评方法	自动化测评
预期结果	不存在随机数不安全使用。
备注	无

5.2.6　数据存储安全

5.2.6.1　内部文件全局读写风险

测评项目	内部文件全局读写风险
风险等级	中危
测评要求	存储敏感信息的文件，如存在账号密码等信息时，不应设置为全局可读写权限。
测评方法	自动化测评
预期结果	不存在内部文件全局读写风险。
备注	无

5.2.6.2　SD 卡数据泄漏风险

测评项目	SD 卡数据泄漏风险
风险等级	中危

测评要求	不应在 SD 卡上存储账号、密码等敏感信息。
测评方法	自动化测评
预期结果	不存在 SD 卡数据泄漏。
备注	无

5.2.6.3　ShardPreference 全局读写风险

测评项目	ShardPreference 全局读写风险
风险等级	中危
测评要求	创建 SharedPreference 时，不应将模式设置为全局读写权限，使用 MODE_PRIVATE 模式。
测评方法	自动化测评
预期结果	不存在 ShardPreference 全局读写风险。
备注	无

5.2.6.4　SQLite 数据库全局读写风险

测评项目	SQLite 数据库全局读写风险
风险等级	中危
测评要求	sqlite 数据库不应设置为全局的可读权限，使用 MODE_PRIVATE 模式。
测评方法	自动化测评
预期结果	不存在 sqlite 数据库全局读写风险。
备注	无

5.2.6.5　SQL 数据库注入风险

测评项目	SQL 数据库注入风险
风险等级	高危
测评要求	构造 SQL 语句，Provider 不需要导出，应将 export 属性设置为 false。
测评方法	自动化测评
预期结果	不存在 SQL 数据库注入风险。
备注	无

5.2.6.6　剪贴板信息泄露风险

测评项目	剪贴板信息泄露风险
风险等级	中危
测评要求	应避免使用剪贴板明文存储敏感信息。
测评方法	自动化测评
预期结果	不存在剪贴板信息泄露。
备注	无

5.2.6.7　应用数据任意备份风险

测评项目	应用数据任意备份风险
风险等级	中危
测评要求	AndroidManifest.xml 文件 application 的属性应设置为 android:allowBackup=“false”。
测评方法	自动化测评
预期结果	不存在应用数据任意备份。
备注	无

5.2.6.8　数据存储位置风险

测评项目	数据存储位置风险

风险等级	高危
测评要求	不应将重要数据存储到 sdcard 目录下。
测评方法	自动化测评
预期结果	不存在数据存储位置风险。
备注	无

5.2.7　组件安全

5.2.7.1　Fragment 注入风险

测评项目	Fragment 注入风险
风险等级	低危
测评要求	PreferenceActivity 的子类中不应加入 isValidFragment 方法，或设置为 false。
测评方法	自动化测评
预期结果	不存在 Fragment 注入风险。
备注	无

5.2.7.2　动态注册广播风险

测评项目	动态注册广播风险
风险等级	高危
测评要求	receiver 调用 registerReceiver()进行动态注册不应采用的全局方式进行注册。
测评方法	自动化测评
预期结果	不存在动态注册广播。
备注	无

5.2.7.3　WebView 组件忽略 SSL 证书验证错误风险

测评项目	WebView 组件忽略 SSL 证书验证错误风险
风险等级	低危
测评要求	不应调用 android.webkit.SslErrorHandler 的 proceed 方法，当发生证书认证错误时，采用默认的处理方法 SslErrorHandler.cancel()
测评方法	自动化测评
预期结果	不存在 WebView 组件忽略 SSL 证书校验错误。
备注	无

5.2.7.4　WebView 密码明文存储风险

测评项目	WebView 密码明文存储风险
风险等级	高危
测评要求	WebView 应将 setSavePassword(true)改为 false。
测评方法	自动化测评
预期结果	不存在 WebView 密码明文存储。
备注	无

5.2.7.5　Activity 最小化权限检测

测评项目	Activity 最小化权限检测
风险等级	中危
测评要求	应设置 Activity 组件最小化特权，即只能自身调用，其他应用无权访问，组件不导出，如果组件必须要进行外部交互，应对组件进行权限控制，增加自定义权限。
测评方法	自动化测评

预期结果	不存在 Activity 最小化权限检测风险。
备注	无

5.2.7.6 Service 最小化权限检测

测评项目	Service 最小化权限检测
风险等级	中危
测评要求	应设置 Service 组件最小化特权，即只能自身调用，其他应用无权访问，组件不导出，如果组件必须要进行外部交互，应对组件进行权限控制，增加自定义权限。
测评方法	自动化测评
预期结果	不存在 Service 最小化权限检测风险。
备注	无

5.2.7.7 Broadcast Receiver 最小化权限检测

测评项目	Broadcast Receiver 最小化权限检测
风险等级	中危
测评要求	应设置 Broadcast Receiver 组件最小化特权，即只能自身调用，其他应用无权访问，组件不导出，如果组件必须要进行外部交互，应对组件进行权限控制，增加自定义权限。
测评方法	自动化测评
预期结果	不存在 Broadcast Receiver 最小化权限检测风险。
备注	无

5.2.7.8 Content Provider 最小化权限检测

测评项目	Content Provider 最小化权限检测
风险等级	中危
测评要求	应设置 Content Provider 组件最小化特权，即只能自身调用，其他应用无权访问，组件不导出，如果组件必须要进行外部交互，应对组件进行权限控制，增加自定义权限。
测评方法	自动化测评
预期结果	不存在 Content Provider 最小化权限检测风险。
备注	无

5.2.7.9 WebView 组件克隆应用漏洞

测评项目	WebView 组件克隆应用漏洞
风险等级	高危
测评要求	若承载 WebView 的 Activity 为可导出，且 webView 支持 File 域，应对导出做校验，否则会存在应用克隆风险，攻击者利用该漏洞，可远程获取用户隐私数据（包括手机应用数据、照片、文档等敏感信息），还可窃取用户登录凭证，在受害者毫无察觉的情况下实现对 APP 用户账户的完全控制。
测评方法	自动化测评
预期结果	不存在 WebView 组件克隆应用漏洞。
备注	无

5.2.7.10 WebView File 域同源策略绕过风险

测评项目	WebView File 域同源策略绕过风险
风险等级	高危
测评要求	应设置 setAllowFileAccess、setAllowFileAccessFromFileURLs 和

	setAllowUniversalAccessFromFileURLs 方法为 false。
测评方法	自动化测评
预期结果	不存在 WebView File 域同源策略绕过风险。
备注	无

5.2.7.11　启用 VPN 服务检测

测评项目	启用 VPN 服务检测
风险等级	低危
测评要求	不应启用 VPN 服务。
测评方法	自动化测评
预期结果	不存在启用 VPN 服务。
备注	无

5.2.7.12　Intent URL Scheme 攻击风险

测评项目	Intent URL Scheme 攻击风险
风险等级	低危
测评要求	不应使用 Intent URL Scheme 格式。
测评方法	自动化测评
预期结果	不存在 Intent URL Scheme 攻击风险
备注	无

5.2.7.13　Intent 隐式调用风险

测评项目	Intent 隐式调用风险
风险等级	中危
测评要求	应使用 Intent.setPackage、Intent.setComponent、Intent.setClassName、Intent.setClass、new Intent(context,Receivered.class)中任一种方法明确指定目标接收方，显式调用 intent。
测评方法	自动化测评
预期结果	不存在 Intent 隐式调用风险
备注	无

5.2.7.14　Webview 远程调试风险

测评项目	Webview 远程调试风险
风险等级	中危
测评要求	WebView.setWebContentsDebuggingEnabled 不应设置为 true，开启 WebView 的远程调试功能，可能会被非法使用者直接利用，获取或者篡改 JS 源代码，从而造成功能逻辑和用户敏感信息泄露。
测评方法	自动化测评
预期结果	不存在 Webview 远程调试风险
备注	无

5.2.7.15　Activity 组件本地拒绝服务

测评项目	Activity 组件本地拒绝服务
风险等级	中危
测评要求	Activity 不应设置导出权限。
测评方法	自动化测评+使用验证
预期结果	不存在 Activity 组件本地拒绝服务风险。
备注	无

5.2.7.16　Service 组件本地拒绝服务

测评项目	Service 组件本地拒绝服务
风险等级	中危
测评要求	Service 不应设置导出权限。
测评方法	自动化测评+使用验证
预期结果	不存在 Service 组件本地拒绝服务风险
备注	无

5.2.7.17　Broadcast Receiver 组件本地拒绝服务

测评项目	Broadcast Receiver 组件本地拒绝服务
风险等级	中危
测评要求	Broadcast Receiver 不应设置导出权限。
测评方法	自动化测评+使用验证
预期结果	不存在 Broadcast Receiver 组件本地拒绝服务风险
备注	无

5.2.7.18　Content Provider SQL 注入风险

测评项目	Content Provider SQL 注入风险
风险等级	高危
测评要求	Content Provider 不应设置导出权限。
测评方法	自动化测评+使用验证
预期结果	不存在 Content Provider SQL 注入风险
备注	无

5.2.7.19　Content Provider 目录遍历风险

测评项目	Content Provider 目录遍历风险
风险等级	高危
测评要求	应将不必要暴露的 Content Provider 组件，设置为私有组件，去除没有必要的 openFile 接口，Content Provider 设置权限级别为 Signature。
测评方法	自动化测评+使用验证
预期结果	不存在 Content Provider 目录遍历风险
备注	无

5.3　漏洞与风险防范检测

5.3.1　恶意攻击防范能力

5.3.1.1　恶意可执行程序感染漏洞

测评项目	恶意可执行程序感染漏洞
风险等级	中危
测评要求	代码中不应包含恶意可执行程序。
测评方法	自动化测评
预期结果	不存在恶意可执行程序感染漏洞。
备注	无

5.3.1.2　运行其它可执行程序漏洞

测评项目	运行其它可执行程序漏洞
风险等级	低危
测评要求	不应运行其它可执行程序。
测评方法	自动化测评

预期结果	不存在应用运行其它可执行程序漏洞。
备注	无

5.3.1.3　本地端口开放越权漏洞

测评项目	本地端口开放越权漏洞
风险等级	低危
测评要求	直接传递命令字或者间接处理有敏感信息或操作时，应避免使用 socket 实现，使用能够控制权限校验身份的方式通讯。
测评方法	自动化测评
预期结果	该应用不存在本地端口开放越权漏洞
备注	无

5.3.1.4　下载任意 apk 风险

测评项目	下载任意 apk 风险
风险等级	中危
测评要求	应对下载 apk 功能的组件调用者进行校验。
测评方法	自动化测评
预期结果	不存在下载任意 apk 风险。
备注	无

5.3.1.5　SO 未使用地址空间随机化风险

测评项目	SO 未使用地址空间随机化风险
风险等级	低危
测评要求	SO 应使用地址空间随机化，如使用 PIE 技术。
测评方法	自动化测评
预期结果	不存在 SO 未使用地址空间随机化风险。
备注	无

5.3.1.6　SO 未使用编译器堆栈保护风险

测评项目	SO 未使用编译器堆栈保护风险
风险等级	低危
测评要求	SO 应使用编译器堆栈保护，如引入 Stack Canaries 漏洞缓解技术。
测评方法	自动化测评
预期结果	不存在 SO 未使用编译器堆栈保护风险。
备注	无

5.3.2　已知漏洞检测

5.3.2.1　FFmpeg 任意文件读取漏洞

测评项目	FFmpeg 任意文件读取漏洞
风险等级	低危
测评要求	不存在 FFmpeg 任意文件读取漏洞（CVE-2016-1897）。
测评方法	自动化测评
预期结果	不存在 FFmpeg 任意文件读取漏洞。
备注	无

5.3.2.2　fastjson 反序列化远程代码执行漏洞

测评项目	fastjson 反序列化远程代码执行漏洞
风险等级	中危
测评要求	不存在 fastjson 反序列化远程代码执行漏洞。

测评方法	自动化测评
预期结果	不存在 fastjson 反序列化远程代码执行漏洞。
备注	无

5.3.2.3　WebView 系统隐藏接口未移除漏洞

测评项目	WebView 系统隐藏接口未移除漏洞
风险等级	中危
测评要求	不存在 WebView 系统隐藏接口漏洞（CVE-2014-1939）。
测评方法	自动化测评
预期结果	不存在 WebView 系统隐藏接口未移除漏洞。
备注	无

5.3.2.4　WebView 组件克隆应用漏洞

测评项目	WebView 组件克隆应用漏洞
风险等级	高危
测评要求	不存在 WebView 组件克隆应用漏洞（CVE-2017-36682）。
测评方法	自动化测评
预期结果	不存在 WebView 组件克隆应用漏洞。
备注	无

5.3.2.5　WebView 组件远程代码执行漏洞

测评项目	WebView 组件远程代码执行漏洞
风险等级	高危
测评要求	不存在 WebView 组件远程代码执行漏洞（CVE-2012-6336）。
测评方法	自动化测评
预期结果	不存在 WebView 组件远程代码执行漏洞。
备注	无

5.3.2.6　"寄生推"SDK 云控漏洞

测评项目	"寄生推"SDK 云控漏洞
风险等级	低危
测评要求	不存在"寄生推"SDK 云控漏洞。
测评方法	自动化测评
预期结果	不存在"寄生推"SDK 云控漏洞。
备注	无

5.3.2.7　ZipperDown 漏洞

测评项目	ZipperDown 漏洞
风险等级	中危
测评要求	不存在 ZipperDown 漏洞。
测评方法	自动化测评
预期结果	不存在 ZipperDown 漏洞。
备注	无

6　iOS 端安全测评要求与方法

6.1　恶意行为

6.1.1　敏感词检测

测评项目	敏感词检测
风险等级	中危
测评要求	不应含有黄赌毒、暴力、宗教、政治、人权等敏感词汇。
测评方法	自动化测评
预期结果	不存在敏感词汇。
备注	无

6.1.2 Private Frameworks 检测

测评项目	Private Frameworks 检测
风险等级	高危
测评要求	不应使用私有库。
测评方法	自动化测评
预期结果	不存在私有库引用。
备注	无

6.1.3 获取前台应用风险

测评项目	获取前台应用风险
风险等级	中危
测评要求	不应有用于前台应用的私有 API。
测评方法	自动化测评
预期结果	不存在获取前台应用信息行为。
备注	无

6.1.4 敏感路径引用风险

测评项目	敏感路径引用风险
风险等级	中危
测评要求	不应访问系统敏感路径，如通话记录数据库、短信数据库、联系人数据库等，进行收集用户信息等行为。
测评方法	自动化测评
预期结果	不存在敏感路径引用风险
备注	无

6.1.5 Private Methods 使用检测

测评项目	Private Methods 使用检测
风险等级	高危
测评要求	不应调用私有库。
测评方法	自动化测评
预期结果	不存在私有 API 调用
备注	无

6.2 安全编译

6.2.1 未使用自动管理内存技术风险

测评项目	未使用自动管理内存技术风险
风险等级	中危
测评要求	应避免内存泄漏，如使用 ARC 技术。
测评方法	自动化测评
预期结果	不存在未使用自动管理内存技术风险
备注	无

6.2.2　未使用编译器堆栈保护器技术

测评项目	未使用编译器堆栈保护器技术
风险等级	中危
测评要求	不应存在缓冲区溢出，使用编译器堆栈保护技术，如 StackGuard 和 SSP，又名 ProPolice。
测评方法	自动化测评
预期结果	不存在未使用编译器堆栈保护技术风险
备注	无

6.3　代码安全

6.3.1　调试日志函数调用风险

测评项目	调试日志函数调用风险
风险等级	低危
测评要求	应在正式版本关闭调试 log 函数输出。
测评方法	自动化测评
预期结果	不存在调试日志函数调用
备注	无

6.3.2　弱加密函数使用风险

测评项目	弱加密函数使用风险
风险等级	低危
测评要求	AES/DES 加密算法，不应选择使用 ECB 或 OFB 工作模式。
测评方法	自动化测评
预期结果	不存在弱加密函数使用
备注	无

6.3.3　弱哈希算法使用风险

测评项目	弱哈希算法使用风险
风险等级	低危
测评要求	不应使用弱哈希算法。
测评方法	自动化测评
预期结果	不存在弱哈希算法使用风险
备注	无

6.3.4　随机数不安全使用风险

测评项目	随机数不安全使用风险
风险等级	中危
测评要求	不应使用可预测的随机数生成器(RNG)。
测评方法	自动化测评
预期结果	不存在随机数不安全使用风险
备注	无

6.3.5　Malloc 方法调用检测

测评项目	Malloc 方法调用检测
风险等级	低危
测评要求	应使用 calloc 替代 malloc 函数。
测评方法	自动化测评
预期结果	不存在 Malloc 方法调用

备注	无

6.3.6　不安全的 API 函数引用风险

测评项目	不安全的 API 函数引用风险
风险等级	低危
测评要求	不应引用不安全的 API 函数，例如未校验字符数组边界造成的缓冲区溢出攻击等漏洞。
测评方法	自动化测评
预期结果	未引用不安全的 API 函数
备注	无

6.3.7　URL 信息泄漏风险

测评项目	URL 信息泄漏风险
风险等级	低危
测评要求	代码内不应存在内部 URL 地址信息。
测评方法	自动化测评
预期结果	不存在 URL 信息泄漏风险
备注	无

6.3.8　资源文件泄露风险

测评项目	资源文件泄露风险
风险等级	低危
测评要求	如 JavaScript 脚本等可能包含资源文件中的重要显示界面及执行，应进行保护处理。
测评方法	自动化测评
预期结果	不存在资源文件泄露风险
备注	无

6.3.9　符号未混淆风险

测评项目	符号未混淆风险
风险等级	低危
测评要求	应通过全局宏定义对自己定义的符号进行混淆保护，给 APP 开发者使用的除外。
测评方法	自动化测评
预期结果	不存在符号未混淆风险
备注	无

6.4　数据存储安全

6.4.1　剪贴板信息泄露风险

测评项目	剪贴板信息泄露风险
风险等级	低危
测评要求	不应把隐私数据，如密码等，存放在剪切板中。
测评方法	自动化测评
预期结果	不存在剪贴板信息泄露风险
备注	无

6.4.2　数据明文存储风险

测评项目	数据明文存储风险
风险等级	低危

测评要求	数据库不应以明文格式存储敏感数据。
测评方法	自动化测评
预期结果	不存在数据明文存储风险
备注	无

6.4.3 配置文件信息明文存储风险

测评项目	配置文件信息明文存储风险
风险等级	低危
测评要求	不应使用 Plist 文件存储明文的用户名、密码等敏感信息。
测评方法	自动化测评
预期结果	不存在配置文件信息明文存储风险
备注	无

6.5 恶意攻击防范

6.5.1 XcodeGhost 感染漏洞

测评项目	XcodeGhost 感染漏洞
风险等级	高危
测评要求	不存在 XcodeGhost 感染漏洞。
测评方法	自动化测评
预期结果	不存在 XcodeGhost 感染漏洞
备注	无

6.5.2 iBackDoor 控制漏洞

测评项目	iBackDoor 控制漏洞
风险等级	高危
测评要求	不存在 iBackDoor 控制漏洞。
测评方法	自动化测评
预期结果	不存在 iBackDoor 控制漏洞
备注	无

6.5.3 ZipperDown 漏洞

测评项目	ZipperDown 漏洞
风险等级	高危
测评要求	不存在 ZipperDown 漏洞。
测评方法	自动化测评
预期结果	不存在 ZipperDown 漏洞
备注	无

6.5.4 YOUMI 恶意 SDK 漏洞

测评项目	YOUMI 恶意 SDK 漏洞
风险等级	中危
测评要求	不存在 YOUMI 恶意 SDK 漏洞。
测评方法	自动化测评
预期结果	不存在 YOUMI 恶意 SDK 漏洞
备注	无

6.5.5 Webview 组件跨域访问漏洞

测评项目	Webview 组件跨域访问漏洞
风险等级	高危

测评要求	不存在 Webview 组件跨域访问漏洞（CNNVD-201801-515）。
测评方法	自动化测评
预期结果	不存在 Webview 组件跨域访问漏洞
备注	无

6.6　数据传输完整性

6.6.1　HTTP 传输数据风险

测评项目	HTTP 传输数据风险
风险等级	高危
测评要求	应使用 HTTPS 传输数据。
测评方法	自动化测评
预期结果	不存在 HTTP 传输数据风险
备注	无

6.6.2　HTTPS 未校验服务器证书风险

测评项目	HTTPS 未校验服务器证书风险
风险等级	中危
测评要求	使用 https 协议时，应在客户端对服务端的身份证书进行完整性校验。
测评方法	自动化测评
预期结果	不存在 HTTPS 未校验服务器证书风险
备注	无

6.6.3　URL Schemes 劫持风险

测评项目	URL Schemes 劫持风险
风险等级	中危
测评要求	不应使用 Intent URL Scheme 格式。
测评方法	自动化测评
预期结果	不存在 URL Schemes 劫持风险
备注	无

7　与 APP 联动测评要求与方法

7.1　非强制

测评项目	非强制
风险等级	低危
测评要求	不应强迫任何单位或组织嵌入互联网广告自动化工具。
测评方法	文档审核
预期结果	不强迫任何单位或组织嵌入互联网广告自动化工具。
备注	无

7.2　安全事件告知

测评项目	安全事件告知
风险等级	低危
测评要求	发现安全风险、安全漏洞、安全事件等时应及时进行更新并告知接入 APP。
测评方法	文档审核
预期结果	发现安全风险、安全漏洞、安全事件等时及时进行更新并告知接入 APP。
备注	无

7.3　个人信息处理规则告知

测评项目	个人信息处理规则告知
风险等级	低危
测评要求	应以明确、易懂、合理的方式向接入APP公开个人信息处理目的、范围、处理方式、处理类型、保存期限、退出方式、需申请的相关权限、问题反馈和投诉渠道等内容，个人信息处理规则变更时应及时进行更新并告知接入APP。
测评方法	文档审核
预期结果	以明确、易懂、合理的方式向接入APP公开个人信息处理目的、范围、处理方式、处理类型、保存期限、退出方式、需申请的相关权限、问题反馈和投诉渠道等内容，个人信息处理规则变更时应及时进行更新并告知接入APP。
备注	无

7.4　第三方代码明示

测评项目	第三方代码明示
风险等级	低危
测评要求	应要求接入APP在其隐私协议中列出互联网广告自动化工具的名称、功能、类型等，及互联网广告自动化工具的隐私协议或收集使用个人信息的类型、目的、方式、范围、退出或关闭方式等。
测评方法	文档审核
预期结果	接入APP在其隐私协议中列出互联网广告自动化工具的名称、功能、类型等，及互联网广告自动化工具的隐私协议或收集使用个人信息的类型、目的、方式、范围、退出或关闭方式等。
备注	无

7.5　个人信息提供

测评项目	个人信息提供
风险等级	低危
测评要求	如接入APP向互联网广告自动化工具提供个人信息，应要求接入APP按照法律法规要求获取用户同意。
测评方法	文档审核
预期结果	1、接入APP不向互联网广告自动化工具提供个人信息； 2、接入APP向互联网广告自动化工具提供个人信息，但接入APP按照法律法规要求获取用户同意。
备注	以上预期结果满足一条即认定为安全。

7.6　广告标识符

测评项目	广告标识符
风险等级	低危
测评要求	互联网广告自动化工具获取广告标识符，应通过接入APP或者终端接口获取广告标识符开关状态，如开关为开启限制则不使用该标识符进行广告推送，如开关为禁止获取广告标识符则不获取广告标识符。
测评方法	文档审核+使用验证
预期结果	通过接入APP或者终端接口获取限制广告跟踪开关状态，且按照开关要求进行限制。
备注	无

7.7　合作协议

测评项目	合作协议
风险等级	低危
测评要求	应与 APP 方签订个人信息处理协议，明确双方相关权利义务、应满足的个人信息安全要求、双方的安全责任及应实施的个人信息安全措施，并妥善留存有关合同和管理记录。
测评方法	文档审核
预期结果	与 APP 方签订个人信息处理协议，明确双方相关权利义务、应满足的个人信息安全要求、双方的安全责任及应实施的个人信息安全措施，并妥善留存有关合同和管理记录。
备注	无

7.8　配合监督

测评项目	配合监督
风险等级	低危
测评要求	APP 开发运营者对接入的第三方服务有监督义务，互联网广告自动化工具应配合 APP 开发运营者的监督。
测评方法	文档审核
预期结果	配合 APP 开发运营者监督。
备注	无

7.9　配合响应

测评项目	配合响应
风险等级	低危
测评要求	应配合接入 APP 及时响应用户请求、申诉等，并妥善留存、及时更新，以供用户查询、使用，如接入 APP 收到个人信息所有者要求，互联网广告自动化工具应配合停止采集处理行为。
测评方法	文档审核
预期结果	配合接入 APP 及时响应用户请求、申诉等，并妥善留存、及时更新，以供用户查询、使用，如接入 APP 收到个人信息所有者要求，配合停止采集处理行为。
备注	无

7.10　安全检测报告

测评项目	安全检测报告
风险等级	低危
测评要求	宜向接入 APP 提供互联网广告自动化工具安全相关检测报告，包括但不限于代码扫描结果（代码审核、加固等证明）、第三方检测机构报告等。
测评方法	文档审核
预期结果	向接入 APP 提供安全相关检测报告，包括但不限于代码扫描结果（代码审核、加固等证明）、第三方检测机构报告等。
备注	本项为建议项

7.11　合作结束

测评项目	合作结束
风险等级	低危
测评要求	当接入 APP 停止接入互联网广告自动化工具后，若互联网广告自动化工具存在从该 APP 共享或收集个人信息的，应删除从该 APP 共享或收集的个人信息或做匿名化处理，或按照合作协议约定处理。

测评方法	文档审核
预期结果	当接入 APP 停止接入互联网广告自动化工具后，互联网广告自动化工具删除从该 APP 共享或收集的个人信息或做匿名化处理，或按照合作协议约定处理。
备注	无

8　隐私协议测评要求与方法

8.1　制定隐私协议

测评项目	制定隐私协议
风险等级	低危
测评要求	应制定隐私协议，隐私协议应清晰、准确、完整地描述个人信息处理规则，并以便于用户阅读、理解的视角，向用户展现可能会对个人权益产生影响的重点内容。
测评方法	文档审核
预期结果	制定隐私协议，并公开个人信息处理规则。
备注	无

8.2　隐私协议内容

测评项目	隐私协议内容
风险等级	低危
测评要求	隐私协议应至少包括适用范围、摘要、收集使用个人信息规则、保障个人信息安全的规则、保障个人信息主体权利的规则、个人信息跨境流动的规则、隐私协议更新的规则等，并提供个人信息处理者的联系方式，且与检测出的敏感行为函数一致。
测评方法	文档审核
预期结果	隐私协议内容完整。
备注	无

8.3　隐私协议公开

测评项目	隐私协议公开
风险等级	低危
测评要求	宜在官方渠道（网站、公众账号等）告知收集、使用个人信息的情况，并提供退出、删除机制。
测评方法	文档审核
预期结果	在官方渠道（网站、公众账号等）告知收集、使用个人信息的情况，并提供退出、删除机制。
备注	本项为建议项

附　录　A
（资料性）
不同格式文件测试项

类型	序号	评测项	AAR	JAR
敏感内容	1	敏感函数检测	✓	✓
	2	敏感词汇检测	✓	✓
源代码安全	1	SO 文件加固检测	✓	
	2	Java 代码混淆检测	✓	✓
	3	日志函数泄漏风险	✓	✓
	4	动态加载 SO 文件风险	✓	✓
	5	测试信息残留风险	✓	✓
	6	URL 硬编码检测	✓	✓
	7	内网测试信息残留漏洞	✓	✓
	8	启动隐藏服务风险	✓	
	9	动态加载 DEX 文件风险	✓	
	10	硬编码风险	✓	✓
	11	单元测试配置风险	✓	
自身安全	1	资源文件泄露风险	✓	
	2	证书明文存储风险	✓	
	3	Java 层动态调试风险	✓	
	4	应用测试模式发布风险	✓	
	5	资源文件包含 APK 检测	✓	
	6	开发商自定义服务风险	✓	
	7	未保护的自定义权限风险	✓	
算法使用安全	1	AES/DES/TDES 加密算法不安全使用风险	✓	✓
	2	RSA 加密算法不安全使用风险	✓	✓
网络通讯安全	1	HTTPS 未校验服务器证书漏洞	✓	✓
	2	HTTPS 未校验主机名风险	✓	✓
	3	HTTPS 允许任意主机名漏洞	✓	✓
	4	传输通道风险	✓	✓
	5	中间人攻击风险	✓	✓
	6	访问境外服务器风险	✓	✓
	7	联网环境检测	✓	✓
数据交互安全	1	getDir 数据全局可读写漏洞	✓	
	2	Intent 敏感数据泄露风险	✓	
	3	PendingIntent 误用 Intent 风险	✓	
	4	发送广播信息泄漏漏洞	✓	
	5	随机数不安全使用风险	✓	✓
数据存储安全	1	内部文件全局读写漏洞	✓	
	2	SD 卡数据泄漏风险	✓	
	3	SharedPreference 全局读写	✓	

类型	序号	评测项	AAR	JAR
		漏洞		
	4	SQLite 数据库全局读写漏洞	✓	
	5	SQL 数据库注入漏洞	✓	
	6	剪贴板信息泄露风险	✓	
	7	应用数据任意备份风险	✓	
	8	数据存储位置风险	✓	
组件安全	1	Fragment 注入漏洞	✓	
	2	动态注册广播风险	✓	
	3	WebView 组件忽略 SSL 证书验证错误漏洞	✓	
	4	WebView 密码明文存储风险	✓	
	5	Activity 最小化权限检测	✓	
	6	Service 最小化权限检测	✓	
	7	Broadcast Receiver 最小化权限检测	✓	
	8	Content Provider 最小化权限检测	✓	
	9	WebView 组件克隆应用漏洞	✓	
	10	WebView File 域同源策略绕过漏洞	✓	
	11	启用 VPN 服务检测	✓	
	12	Intent URL Scheme 攻击漏洞	✓	
	13	Intent 隐式调用风险	✓	
	14	Webview 远程调试风险	✓	
	15	Activity 组件本地拒绝服务	✓	✓
	16	Service 组件本地拒绝服务	✓	✓
	17	Broadcast Receiver 组件本地拒绝服务	✓	✓
	18	Content Provider SQL 注入风险	✓	✓
	19	Content Provider 目录遍历风险	✓	✓
恶意攻击防范能力	1	恶意可执行程序感染漏洞	✓	
	2	运行其它可执行程序漏洞	✓	✓
	3	本地端口开放越权漏洞	✓	✓
	4	下载任意 apk 风险	✓	
	5	SO 未使用地址空间随机化风险	✓	
	6	SO 未使用编译器堆栈保护风险	✓	
已知漏洞检测	1	FFmpeg 任意文件读取漏洞	✓	
	2	fastjson 反序列化远程代码执行漏洞	✓	✓
	3	WebView 系统隐藏接口未移除漏洞	✓	
	4	WebView 组件克隆应用漏洞	✓	
	5	WebView 组件远程代码执行漏	✓	

类型	序号	评测项	AAR	JAR
		洞		
	6	"寄生推"SDK 云控漏洞	✓	✓
	7	ZipperDown 漏洞	✓	✓

类型	序号	评测项	dylib	framework	a
恶意行为	1	敏感词检测		✓	
	2	Private Frameworks 检测	✓		
	3	敏感路径引用风险	✓	✓	✓
	4	获取前台应用风险		✓	✓
	5	Private Methods 使用检测	✓	✓	
安全编译	1	未使用自动管理内存技术风险	✓		
	2	未使用编译器堆栈保护技术风险	✓		
代码安全	1	调试日志函数调用风险	✓	✓	✓
	2	弱加密函数使用风险	✓	✓	✓
	3	弱哈希算法使用风险	✓	✓	✓
	4	随机数不安全使用风险	✓	✓	✓
	5	Malloc 方法调用检测	✓	✓	✓
	6	不安全的 API 函数引用风险	✓	✓	✓
	7	URL 信息泄漏风险	✓	✓	✓
	8	资源文件泄露风险		✓	
	9	符号未混淆风险	✓		
数据存储安全	1	剪贴板信息泄露风险	✓	✓	✓
	2	数据库明文存储风险	✓	✓	✓
	3	配置文件信息明文存储风险		✓	
恶意攻击防范	1	XcodeGhost 感染漏洞	✓	✓	✓
	2	iBackDoor 控制漏洞	✓	✓	✓
	3	ZipperDown 漏洞	✓	✓	✓
	4	YOUMI 恶意 SDK 漏洞	✓	✓	✓
	5	Webview 组件跨域访问风险	✓	✓	✓
数据传输完整性	1	HTTP 传输数据风险	✓	✓	
	2	HTTPS 未校验服务器证书漏洞	✓		
	3	URL Schemes 劫持风险		✓	

附　录　B
（资料性）
文档审核记录表

测试序号	1
测 试 类	与 APP 联动测评
测 试 项	非强制
测试要求： 不应强迫任何单位或组织嵌入互联网广告自动化工具。	
测试内容： 1. 访谈对接人员，是否所有单位或组织都是自愿嵌入的。	
测试记录： 1. 是否所有单位或组织都是自愿嵌入？ ☐ 否　　☐ 是	
备注：	

测试序号	2
测 试 类	与 APP 联动测评
测 试 项	安全事件告知
测试要求： 发现安全风险、安全漏洞、安全事件等时应及时进行更新并告知接入 APP。	
测试内容： 1.当发现安全风险、安全漏洞、安全事件等时如何进行更新，提供内部的流程文档等证明材料； 2.当发现安全风险、安全漏洞、安全事件等时是否将更新或解决办法告知接入 APP，提供与 APP 间的合同等证明材料。	
测试记录： 1. 发现安全风险、安全漏洞、安全事件等时是否及时进行更新？ ☐ 否　　☐ 是：_____ 2. 发现安全风险、安全漏洞、安全事件等时是否时进行告知接入 APP？ ☐ 否　　☐ 是：_____	
备注：	

测试序号	3
测 试 类	与 APP 联动测评
测 试 项	个人信息处理规则告知
测试要求： 应以明确、易懂、合理的方式向接入APP公开个人信息处理目的、范围、处理方式、处理类型、保存期限、退出方式、需申请的相关权限、问题反馈和投诉渠道等内容，个人信息处理规则变更时应及时进行更新并告知接入APP。	
测试内容： 1. 查看公开的隐私条款或其他证明材料，是否以明确、易懂、合理的方式向接入 APP 公开个人信息处理目的、范围、处理方式、处理类型、保存期限、退出方式、需申请的相关权限、问题反馈和投诉渠道等内容； 2. 个人信息处理规则变更时是否及时进行更新并告知接入 APP，提供证明文件。	
测试记录：	

1. 是否是以明确、易懂、合理的方式向接入 APP 公开个人信息处理目的、范围、处理方式、处理类型、保存期限、退出方式、需申请的相关权限、问题反馈和投诉渠道等内容？ ☐ 否　　☐ 是：_____ 2. 个人信息处理规则变更时是否及时进行更新并告知接入 APP？ ☐ 否　　☐ 是：_____
备注：

测试序号	4
测 试 类	与 APP 联动测评
测 试 项	第三方代码明示
测试要求： 应要求接入APP在其隐私协议中列出互联网广告自动化工具的名称、功能、类型等，及互联网广告自动化工具的隐私协议或收集使用个人信息的类型、目的、方式、范围、退出或关闭方式等。	
测试内容： 1. 是否要求接入 APP 在其隐私协议中列出本 SDK 的名称、功能、类型等； 2. 是否要求接入 APP 在其隐私协议中列出本 SDK 的隐私协议或收集使用个人信息的类型、目的、方式、范围、退出或关闭方式等； 3. 查看已接入 APP 的隐私协议，验证是否在其隐私协议中列出相应内容。	
测试记录： 1. 是否要求接入 APP 在其隐私协议中列出本 SDK 的名称、功能、类型等？ ☐ 否　　☐ 是 2. 是否要求列出本 SDK 的隐私协议或收集使用个人信息的类型、目的、方式、范围、退出或关闭方式等？ ☐ 否　　☐ 是 3. 接入 APP 的隐私协议是否在其隐私协议中列出相应内容？ ☐ 否　　☐ 是：_____	
备注：	

测试序号	5
测 试 类	与 APP 联动测评
测 试 项	个人信息提供
测试要求： 如接入APP向互联网广告自动化工具提供个人信息，应要求接入APP按照法律法规要求获取用户同意。	
测试内容： 1. 是否有接入 APP 向互联网广告自动化工具提供个人信息； 2. 如有，是否要求接入 APP 按照法律法规要求获取用户同意。	
测试记录： 1. 是否有接入 APP 向本 SDK 提供个人信息？ ☐ 否　　☐ 是：是否要求接入 APP 按照法律法规要求获取用户同意？ ☐ 否　　☐ 是：_____	
备注：	

测试序号	6
测 试 类	与 APP 联动测评

测 试 项	广告标识符
测试要求： 互联网广告自动化工具获取广告标识符，应通过接入APP或者终端接口获取广告标识符开关状态，如开关为开启限制则不使用该标识符进行广告推送，如开关为禁止获取广告标识符则不获取广告标识符。	
测试内容： 1. 查看文档，是否列出获取广告标识的类型； 2. 是通过接入 APP 获取还是自行获取； 3. 是否获取广告标识符开关状态； 4. 是否按照开关要求进行限制。	
测试记录： 1. 是否列出获取广告标识的类型？ ☐ 否　　☐ 是：_____ 2. 是通过接入 APP 获取还是自行获取？ ☐ 接入 APP　　☐ 自行获取 3. 是否获取广告标识符开关状态？ ☐ 否　　☐ 是：_____ 4. 是否按照开关要求进行限制？ ☐ 否　　☐ 是：_____	
备注：	

测试序号	7
测 试 类	与 APP 联动测评
测 试 项	合作协议
测试要求： 应与APP方签订个人信息处理协议，明确双方相关权利义务、应满足的个人信息安全要求、双方的安全责任及应实施的个人信息安全措施，并妥善留存有关合同和管理记录。	
测试内容： 1. 查看是否与 APP 方签订个人信息处理协议； 2. 查看协议是否明确双方相关权利义务、应满足的个人信息安全要求、双方的安全责任及应实施的个人信息安全措施； 3. 是否有留存有关合同和管理记录。	
测试记录： 1. 是否与 APP 方签订个人信息处理协议？ ☐ 否　　☐ 是：_____ 2. 协议是否明确双方相关权利义务、满足的个人信息安全要求、双方的安全责任及实施的个人信息安全措施？ ☐ 否　　☐ 是：_____ 3. 是否有留存有关合同和管理记录？ ☐ 否　　☐ 是	
备注：	

测试序号	8
测 试 类	与 APP 联动测评
测 试 项	配合监督
测试要求： APP开发运营者对接入的第三方服务有监督义务，互联网广告自动化工具应配合APP开发运营者的	

监督。
测试内容： 1.是否有 APP 开发运营者对本 SDK 进行监督、技术检测等； 2.如有，是否配合 APP 开发运营者对本 SDK 的监督、技术检测等，并提供相应证明材料；如无，是否有内部流程文件要求配合。
测试记录： 1. 是否有 APP 开发运营者对本 SDK 进行监督、技术检测等？ ☐否：是否有内部流程文件要求配合？ ☐ 否　　☐ 是：_____ ☐是：是否配合 APP 开发运营者对本 SDK 的监督、技术检测等？ ☐ 否　　☐ 是：_____
备注：

测试序号	9
测 试 类	与 APP 联动测评
测 试 项	配合响应
测试要求： 应配合接入APP及时响应用户请求、申诉等，并妥善留存、及时更新，以供用户查询、使用，如接入APP收到个人信息所有者要求，互联网广告自动化工具应配合停止采集处理行为。	
测试内容： 1.是否有接入 APP 提出响应用户请求、申诉等； 2.如有，是否配合 APP 响应用户请求、申诉等，并妥善留存、及时更新，并提供相应证明材料；如无，访谈对接人员，询问是否有内部流程文件要求配合； 3.是否有接入 APP 收到个人信息所有者要求停止采集； 4.如有，是否配合停止采集处理行为，并提供相应证明材料；如无，访谈对接人员，询问是否有内部流程文件要求配合。	
测试记录： 1. 是否有接入 APP 提出响应用户请求、申诉等？ ☐否：是否有内部流程文件要求配合？ ☐ 否　　☐ 是：_____ ☐是：是否配合 APP 响应用户请求、申诉等，并妥善留存、及时更新？ ☐ 否　　☐ 是：_____ 2. 是否有接入 APP 收到个人信息所有者要求停止采集? ☐否：是否有内部流程文件要求配合？ ☐ 否　　☐ 是：_____ ☐是：是否配合停止采集处理行为? ☐ 否　　☐ 是：_____	
备注：	

测试序号	10
测 试 类	与 APP 联动测评
测 试 项	安全检测报告
测试要求： 宜向接入APP提供互联网广告自动化工具安全相关检测报告，包括但不限于代码扫描结果（代码审核、加固等证明）、第三方检测机构报告等。	

测试内容： 1.是否向接入 APP 提供互联网广告自动化工具安全相关检测报告,包括但不限于代码扫描结果(代码审核、加固等证明)、第三方检测机构报告等。
测试记录： 1. 是否向接入 APP 提供互联网广告自动化工具安全相关检测报告，包括但不限于代码扫描结果（代码审核、加固等证明）、第三方检测机构报告等？ □否　　□是：_____
备注：

测试序号	11
测 试 类	与 APP 联动测评
测 试 项	合作结束
测试要求： 当接入APP停止接入互联网广告自动化工具后，若互联网广告自动化工具存在从该APP共享或收集个人信息的，应删除从该APP共享或收集的个人信息或做匿名化处理，或按照合作协议约定处理。	
测试内容： 1.是否有 APP 停止接入 SDK，且 SDK 存在从该 APP 共享或收集的个人信息； 2.如有，是否合作协议约定删除或处理方式，且按照合作协议约定，删除从该 App 共享或收集的个人信息或做匿名化处理；如无，访谈对接人员，查看与 APP 的合作协议是否约定删除或处理方式。	
测试记录： 1. 是否有 APP 停止接入 SDK，且 SDK 存在从该 APP 共享或收集的个人信息？ □否：与 APP 的合作协议是否约定删除或处理方式？ □ 否　　□ 是：_____ □是：是否合作协议约定删除或处理方式，且按照合作协议约定，删除从该 APP 共享或收集的个人信息或做匿名化处理？ □ 否　　□ 是：_____	
备注：	

测试序号	12
测 试 类	隐私协议
测 试 项	制定隐私协议
测试要求： 应制定隐私协议，隐私协议应清晰、准确、完整地描述个人信息处理规则，并以便于用户阅读、理解的视角，向用户展现可能会对个人权益产生影响的重点内容。	
测试内容： 1. 是否制定并公开隐私协议； 2. 隐私协议是否清晰、准确、完整地描述个人信息处理规则，并以便于用户阅读、理解的视角，向用户展现可能会对个人权益产生影响的重点内容。	
测试记录： 1. 是否制定并公开隐私协议？ □ 否　　□ 是：_____ 2. 隐私协议是否清晰、准确、完整地描述个人信息处理规则，并以便于用户阅读、理解的视角，向用户展现可能会对个人权益产生影响的重点内容？ □ 否　　□ 是：_____	
备注：	

测试序号	13
测 试 类	隐私协议
测 试 项	隐私协议内容
测试要求： 隐私协议应至少包括适用范围、摘要、收集使用个人信息规则、保障个人信息安全的规则、保障个人信息主体权利的规则、个人信息跨境流动的规则、隐私协议更新的规则等，并提供个人信息处理者的联系方式，且与检测出的敏感行为函数一致。	
测试内容： 1. 隐私协议是否包括适用范围、摘要、收集使用个人信息规则、保障个人信息安全的规则、保障个人信息主体权利的规则、个人信息跨境流动的规则、隐私协议更新的规则等，并提供个人信息处理者的联系方式； 2. 隐私协议是否与检测出的敏感行为函数一致。	
测试记录： 1. 是否包括适用范围、摘要、收集使用个人信息规则、保障个人信息安全的规则、保障个人信息主体权利的规则、个人信息跨境流动的规则、隐私协议更新的规则等，并提供个人信息处理者的联系方式？ □ 否　　□ 是：_____ 2. 是否与检测出的敏感行为函数一致？ □ 否　　□ 是：_____	
备注：	

测试序号	14
测 试 类	隐私协议
测 试 项	隐私协议公开
测试要求： 宜在官方渠道（网站、公众账号等）告知收集、使用个人信息的情况，并提供退出、删除机制。	
测试内容： 1. 是否在其官方渠道（网站、公众账号等）告知收集、使用个人信息的情况； 2. 是否在其官方渠道（网站、公众账号等）告知退出、删除机制。	
测试记录： 1. 是否在其官方渠道（网站、公众账号等）告知收集、使用个人信息的情况？ □ 否　　□ 是：_____ 2. 是否在其官方渠道（网站、公众账号等）告知退出、删除机制？ □ 否　　□ 是：_____	
备注：	

参 考 文 献

[1]中华人民共和国网络安全法[Z].2016.
[2]中华人民共和国数据安全法[Z].2021.
[3]中华人民共和国个人信息保护法[Z].2021.
[4]APP违法违规收集使用个人信息行为认定方法:国信办秘字〔2019〕191号[Z].2019.
[5]信息安全技术 个人信息安全规范:GB/T 35273-2020[S].2020.
[6]信息安全技术 移动互联网应用程序（App）收集个人信息基本规范:GB/T 41391-2022[S].2022.
[7]信息安全技术 个人信息告知同意指南:GB/T 42574-2023[S].2023.
[8]信息安全技术 移动互联网应用程序（APP）个人信息安全测评规范:GB/T 42582-2023[S].2023.
[9]信息安全技术 移动互联网应用程序（App）软件开发工具包（SDK）安全要求:GB/T 43435-2023[S].2023.
[10]网络安全标准实践指南—移动互联网应用程序(App)收集使用个人信息自评估指南:TC260-PG-20202A[S].2020.
[11]网络安全标准实践指南—移动互联网应用程序（App）个人信息保护常见问题及处置指南:TC260-PG-20203A[S].2020.
[12]网络安全标准实践指南—移动互联网应用程序（App）使用软件开发工具包（SDK）安全指引:TC260-PG-20205A[S].2020.
[13]互联网广告数据应用和安全技术要求:TCAAAD 001-2021/TCCSA 329-2021[S].2021.
[14]移动智能终端应用软件SDK安全技术要求:TAF-WG4-AS0057-V1.0.0 2020[S].2020.