南明离火

移动应用检测平台

ANDROID 静态分析报告

Surah Shiksha • v1.0.6

分析日期: 2025-08-04 08:09:07

应用概览

文件名称:	Surah Shiksha v1.0.6.apk
文件大小:	11.98MB
应用名称:	Surah Shiksha
软件包名:	com.shahriar.surahshikkha
主活动:	com.shahriar.surahshikkha.UI.SplashActivity
版本号:	1.0.6
最小SDK:	21
目标SDK:	34
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	67/100 (低风险)
杀软检测:	经检测，该文件安全
MD5:	43957652bc7f37f570fec046f3db75b7
SHA1:	ddfc2aaaf4723e86936b127ca09cecb16e6885f8
SHA256:	9ba2355bdeffcf065f560242bec8ada855256685e7431f77caaee0aecac56e

分析结果严重性分布

高危	中危	信息	安全	关注
0	3	1	1	0

四大组件导出状态统计

Activity组件：3个，其中export的有： 1个
Service组件：0个，其中export的有： 0个
Receiver组件：1个，其中export的有： 1个
Provider组件：1个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2018-06-09 17:20:57+00:00
有效期至: 2048-06-09 17:20:57+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0x3bc1787c30438b13ab8edf39103f3ead3fdd4d1d
哈希算法: sha256
证书MD5: 409c4e405482a46294497043c8f1177f
证书SHA1: fbde44d8b1c66b0af28b647556c02b1ec1e1af25
证书SHA256: 4864cf2c1b35d1ed96841edfa8bc478dcea10db0b7965e70e2c41767d464a8c1
证书SHA512:
0b1913515f3603cc7d40096bf5ab11f521162b26a48adaeda270401e85577de6b8215ff5001978403c801dbc479c031c6b25908dc2267e322beeb42fcc20d26

公钥算法: rsa
密钥长度: 4096
指纹: ca673b8495520a61d25ffba22fe228ff25add3d8f479cf89df7fdc8a94025d8b
共检测到 1 个唯一证书

权限声明与风险分级

权限名称	安全等级	权限内容	权限描述
com.shahriar.surahshikkha.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

网络通信安全风险分析

序号	范围	严重级别	描述

证书安全合规分析

高危: 0 | 警告: 1 | 信息: 1

标题	严重程度	描述信息
已签名应用	信息	应用已使用代码签名证书进行签名。

Manifest 配置安全分析

高危: 0 | 警告: 2 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息

1	Activity (com.shahriar.surahshikkha.UI.DashboardActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
2	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。

代码安全漏洞检测

高危: **0** | 警告: **1** | 信息: **1** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	应用程序记录日志信息,不得记录敏感信息	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限
2	应用程序使用不安全的随机数生成器	警告	CWE: CWE-330: 使用不充分的随机数 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	升级会员：解锁高级权限

应用行为分析

编号	行为	标签	文件
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00024	Base64解码后写入文件	反射 文件	升级会员：解锁高级权限
00104	检查给定路径是否是目录	文件	升级会员：解锁高级权限
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限

敏感权限滥用分析

类型	匹配	权限

恶意软件常用权限	0/30	
其它常用权限	0/46	

常用: 已知恶意软件广泛滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

URL 链接安全分析

URL信息	源码文件
• https://play.google.com/store/apps/details?id= • http://play.google.com/store/apps/details?id=	r0/f.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Jetpack App Startup	Google	App Startup 库提供了一种直接，高效的方法来在应用程序启动时初始化组件。库开发人员和应用程序开发人员都可以使用 App Startup 来简化启动顺序并显式设置初始化顺序。App Startup 允许您定义共享单个内容提供程序的组件初始化程序，而不必为需要初始化的每个组件定义单独的内容提供程序。这可以大大缩短应用启动时间。
Jetpack ProfileInstaller	Google	让库能够提前访问要由 ART 读取的编译轨迹。

免责声明及风险提示:

本报告由南明离火移动安全分析平台自动生成，内容仅供参考，不构成任何法律意见或建议。本平台对使用本产品及其内容所引发的任何直接或间接损失概不负责。本报告内容仅供网络安全研究，不得违反中华人民共和国相关法律法规。如有任何疑问，请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动端恶意软件分析和安全评估框架。它能够执行静态分析和动态分析，深入扫描软件中中潜在的漏洞和安全隐隐患。