



ANDROID 静态分析报告



IVOJI • v3.0.13

分析日期: 2024-07-17 10:40:54

i应用概览

文件名称:	id.ivoji_2024-04-16.apk
文件大小:	12.94MB
应用名称:	IVOJI
软件包名:	id.ivoji
主活动:	com.ivoji.commonlibrary.ui.WelcomeActivity
版本号:	3.0.13
最小SDK:	21
目标SDK:	33
加固信息:	未加壳
应用程序安全分数:	35/100 (高风险)
跟踪器检测:	7/432
杀软检测:	AI评估: 安全
MD5:	b01615297ea3980e3e9dec7291a5125a
SHA1:	106c2156677b7960ef64a58a7a3a79c49ea4ecc4
SHA256:	f942c671c444768a7101572874bfd2b865002a551b289f0989ba2079b36ca0c

📊分析结果严重性分布

🚨 高危	⚠️ 中危	ℹ️ 信息	✅ 安全	🔍 关注
3	2	1	0	7

📦四大组件导出状态统计

Activity组件: 13个, 其中export的有: 1个
Service组件: 11个, 其中export的有: 1个
Receiver组件: 6个, 其中export的有: 1个
Provider组件: 3个, 其中export的有: 0个

🔑应用签名证书信息

二进制文件已签名

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: 2020-02-29 13:51:38+00:00
有效期至: 2050-02-28 13:51:38+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xb67829f637a98860fd017c9aa1702733c34b9758
哈希算法: sha256
证书MD5: 2ae30e9d33250c52acd1b294b63fdee8
证书SHA1: ed7e00b851908e1f6c24a952d552355366a61c97
证书SHA256: b47965de1c5e3d057f2d83dc186fc081fa370974ade3e0f5023a82e354600e56
证书SHA512:
a08840d83fe4b1020bf53e7a443367b99158b76fd08589d3f937c78fb124fc8e660e9a41a50afc81cd7ea062b9c4156f49b11470dd68296886e8ba1ba879dfd9

公钥算法: rsa
密钥长度: 4096
指纹: 21939677b2778050731cdfa6ad1177c45b013d46723521c06fc6b80fc62b10aa
找到 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
android.permission.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
android.permission.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户错略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
android.permission.ACCESS_NETWORK_STATE	普通	获取网络状态	允许应用程序查看所有网络的状态。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。
android.permission.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
android.permission.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
android.permission.HIGH_SAMPLING_RATE_SENSORS	普通	传感器的数据刷新率限制	允许应用以大于 200 Hz 的采样率访问传感器数据，此数据包括由设备的加速度，陀螺仪和磁力传感器记录的值。
android.permission.ACCESS_AD SERVICES_ATTRIBUTION	普通	允许应用程序访问广告服务归因	这使应用能够检索与广告归因相关的信息，这些信息可用于有针对性的广告目的。应用程序可以收集有关用户如何与广告互动的数据，例如点击或展示，以衡量广告活动的有效性。
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。
android.permission.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。
com.google.android.gms.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。
id.ivoji.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.facebook.CustomTabActivity	Schemes: @string/FACEBOOK_LOGIN_SCHEMA://, fbconnect://, Hosts: cct.id.ivoji,

网络通信安全风险分析

高危: 1 | 警告: 0 | 信息: 0 | 安全: 0

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。

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	应用程序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: 4 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 5.0-5.0.2, [minSdk=21]	信息	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。
2	应用程序具有网络安全配置 [android:networkSecurityConfig="@xml/network_security_config"]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
3	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。
4	Activity (com.facebook.CustomTabActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
5	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护，但是应该检查权限的保护级别。 Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

6	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序, 因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此, 应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险, 一个恶意应用程序可以请求并获得这个权限, 并与该组件交互。如果它被设置为签名, 只有使用相同证书签名的应用程序才能获得这个权限。
---	--	----	--

</> 代码安全漏洞检测

高危: 1 | 警告: 2 | 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	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员: 解锁高级权限
3	该文件是World Readable。任何应用程序都可以读取文件	高危	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员: 解锁高级权限
4	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

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY (栈保护)	RELRO	RPATH (指定SO搜索路径)	RUNPATH (指定SO搜索路径)	FORTIFY(常用函数加强检查)	SYMBOLSSTRIPPED(裁剪符号表)
1	arm64-v8a/libbd_unifylicense.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT (.got 和 .got.plt 两者) 被标记为只读。	No info 二进制文件没有设置运行时搜索路径或 RPATH	No info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 libc 的常见不安全函数（如 strcpy, gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/FIutter 库不适用	False warning 符号可用

2	arm64-v8a/libk5V5Ll8r01joxQG.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	No ne info 二进制文件没有设置运行时搜索路径或 RPATH	No ne info 二进制文件没有设置 RUNPATH	True info 二进制文件有以下加固函数: [__vsprintf_chk', '__vsprintf_chk']	False warning 符号可用
3	arm64-v8a/libpaddle_light_api_shared.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	No ne info 二进制文件没有设置运行时搜索路径或 RPATH	No ne info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 libc 的常见不安全函数（如 strcpy, gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/FIutter 库不适用	False warning 符号可用

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	3/56	android.permission.ACCESS_COARSE_LOCATION android.permission.WAKE_LOCK android.permission.CAMERA
其它常用权限	5/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE com.google.android.gms.permission.AD_ID com.google.android.c2dm.permission.RECEIVE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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。

🔍 恶意域名威胁检测

域名	状态	中国境内	位置信息
scdn-stestsettings.s	安全	否	No Geolocation information available.
app.adjust.cn	安全	是	IP地址: 47.104.30.117 国家: 中国 地区: 山东 城市: 青岛 纬度: 36.098610 经度: 120.371941 查看: 高德地图
pagead2.google syndication.com	安全	是	IP地址: 180.163.151.166 国家: 中国 地区: 上海 城市: 上海 纬度: 31.224233 经度: 121.465948 查看: 高德地图
sregister.s	安全	否	No Geolocation information available.
sonelink.s	安全	否	No Geolocation information available.
graph-video.s	安全	否	No Geolocation information available.
sapp.s	安全	否	No Geolocation information available.
smonitorsdk.s	安全	否	No Geolocation information available.
subscription.eu.adjust.com	安全	否	IP地址: 185.151.204.60 国家: 美利坚合众国 地区: 加利福尼亚 城市: 丘珀蒂诺 纬度: 37.323002 经度: -122.032181 查看: Google 地图
scdn-ssettings.s	安全	否	No Geolocation information available.
app.eu.adjust.com	安全	否	IP地址: 185.151.204.60 国家: 美利坚合众国 地区: 加利福尼亚 城市: 丘珀蒂诺 纬度: 37.323002 经度: -122.032181 查看: Google 地图
google.com	安全	是	IP地址: 172.217.161.78 国家: 中国 地区: 香港 城市: 香港 纬度: 22.285521 经度: 114.157692 查看: 高德地图

subscription.adjust.net.in	安全	否	IP地址: 185.151.204.51 国家: 美利坚合众国 地区: 加利福尼亚 城市: 丘珀蒂诺 纬度: 37.323002 经度: -122.032181 查看: Google 地图
sconversions.s	安全	否	No Geolocation information available.
subscription.adjust.com	安全	否	IP地址: 185.151.204.52 国家: 美利坚合众国 地区: 加利福尼亚 城市: 丘珀蒂诺 纬度: 37.323002 经度: -122.032181 查看: Google 地图
login.live.com	安全	否	IP地址: 40.126.35.144 国家: 新加坡 地区: 新加坡 城市: 新加坡 纬度: 1.289987 经度: 103.850231 查看: Google 地图
subscription.adjust.world	安全	否	IP地址: 185.151.204.44 国家: 美利坚合众国 地区: 加利福尼亚 城市: 丘珀蒂诺 纬度: 37.323002 经度: -122.032181 查看: Google 地图
app.adjust.net.in	安全	否	IP地址: 185.151.204.51 国家: 美利坚合众国 地区: 加利福尼亚 城市: 丘珀蒂诺 纬度: 37.323002 经度: -122.032181 查看: Google 地图
svalidate.s	安全	否	No Geolocation information available.
gdpr.eu.adjust.com	安全	否	IP地址: 185.151.204.60 国家: 美利坚合众国 地区: 加利福尼亚 城市: 丘珀蒂诺 纬度: 37.323002 经度: -122.032181 查看: Google 地图
app-measurement.com	安全	是	IP地址: 180.163.150.161 国家: 中国 地区: 上海 城市: 上海 纬度: 31.224333 经度: 121.468948 查看: 高德地图
gdpr.us.adjust.com	安全	否	No Geolocation information available.
gdpr.tr.adjust.com	安全	否	No Geolocation information available.

graph.s	安全	否	No Geolocation information available.
sinapps.s	安全	否	No Geolocation information available.
aps-webhandler.appsflyer.com	安全	否	No Geolocation information available.
sars.s	安全	否	No Geolocation information available.
www.linkedin.com	安全	是	IP地址: 52.130.75.155 国家: 中国 地区: 上海 城市: 上海 纬度: 31.224333 经度: 121.468948 查看: 高德地图
sadrevenue.s	安全	否	No Geolocation information available.
sattr.s	安全	否	No Geolocation information available.
gdpr.adjust.com	安全	否	IP地址: 35.201.97.85 国家: 美利坚合众国 地区: 加利福尼亚州 城市: 丘珀蒂诺 纬度: 37.323603 经度: -122.032181 查看: Google 地图
ssdk-services.s	安全	否	No Geolocation information available.
slaunches.s	安全	否	No Geolocation information available.
ivoji-001.firebaseio.com	安全	否	IP地址: 35.201.97.85 国家: 美利坚合众国 地区: 密苏里州 城市: 堪萨斯城 纬度: 39.099731 经度: -94.578568 查看: Google 地图
appv.ivoji.id	安全	否	IP地址: 195.244.54.5 国家: 印度尼西亚 地区: 雅加达雷亚 城市: 雅加达 纬度: -6.208678 经度: 106.845490 查看: Google 地图
www.googletagmanager.com	安全	是	IP地址: 180.163.150.41 国家: 中国 地区: 上海 城市: 上海 纬度: 31.224333 经度: 121.468948 查看: 高德地图

subscription.us.adjust.com	安全	否	IP地址: 185.151.204.70 国家: 美利坚合众国 地区: 加利福尼亚 城市: 丘珀蒂诺 纬度: 37.323002 经度: -122.032181 查看: Google 地图
aip.baidubce.com	安全	是	IP地址: 180.97.107.95 国家: 中国 地区: 江苏 城市: 苏州 纬度: 31.311365 经度: 120.617691 查看: 高德地图
gdpr.adjust.world	安全	否	IP地址: 185.151.204.40 国家: 美利坚合众国 地区: 加利福尼亚 城市: 丘珀蒂诺 纬度: 37.323002 经度: -122.032181 查看: Google 地图
app.tr.adjust.com	安全	否	IP地址: 195.244.54.5 国家: 土耳其 地区: 伊兹密尔 城市: 伊兹密尔 纬度: 38.412731 经度: 27.138380 查看: Google 地图
gdpr.adjust.net.in	安全	否	IP地址: 185.151.204.32 国家: 美利坚合众国 地区: 加利福尼亚 城市: 丘珀蒂诺 纬度: 37.323002 经度: -122.032181 查看: Google 地图
subscription.tr.adjust.com	安全	否	IP地址: 195.244.54.6 国家: 土耳其 地区: 伊兹密尔 城市: 伊兹密尔 纬度: 38.412731 经度: 27.138380 查看: Google 地图
facebook.com	安全	否	IP地址: 157.240.31.35 国家: 日本 地区: 东京 城市: 东京 纬度: 35.689499 经度: 139.692322 查看: Google 地图
sgcdsdk.s	安全	否	No Geolocation information available.

www.paypal.com	安全	否	IP地址: 146.75.49.21 国家: 瑞典 地区: 西约塔兰省 城市: 哥德堡 纬度: 57.707409 经度: 11.966732 查看: Google 地图
simpression.s	安全	否	No Geolocation information available.
login.yahoo.com	安全	否	IP地址: 124.108.115.75 国家: 台湾省 地区: 台北 城市: 台北 纬度: 25.038172 经度: 121.565599 查看: Google 地图
sdlSDK.s	安全	否	No Geolocation information available.
twitter.com	安全	否	IP地址: 104.244.42.193 国家: 美利坚合众国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.773958 经度: -122.410446 查看: Google 地图
sviap.s	安全	否	No Geolocation information available.
app.adjust.com	安全	否	IP地址: 185.151.204.15 国家: 美利坚合众国 地区: 加利福尼亚 城市: 丘珀蒂诺 纬度: 37.323002 经度: -122.032181 查看: Google 地图
app.us.adjust.com	安全	否	IP地址: 185.151.204.70 国家: 美利坚合众国 地区: 加利福尼亚 城市: 丘珀蒂诺 纬度: 37.323002 经度: -122.032181 查看: Google 地图
goo.gl	安全	否	IP地址: 142.251.42.174 国家: 印度 地区: 马哈拉施特拉邦 城市: 孟买 纬度: 19.075975 经度: 72.877380 查看: Google 地图
app.adjust.world	安全	否	IP地址: 185.151.204.43 国家: 美利坚合众国 地区: 加利福尼亚 城市: 丘珀蒂诺 纬度: 37.323002 经度: -122.032181 查看: Google 地图

🌐 URL 链接安全分析

URL信息	源码文件
- https://%scdn-%stestsettings.%s/android/v1/%s/settings - https://%scdn-%ssettings.%s/android/v1/%s/settings	com/appsflyer/internal/AFe1gSDK.java
- https://%sattr.%s/api/v - https://%slaunches.%s/api/v - https://%sconversions.%s/api/v - https://aps-webhandler.appsflyer.com/api/trigger - https://%sadrevenue.%s/api/v2/log/adimpression/v6.13.1/android?app_id= - https://%svalidate.%s/api/v - https://%ssdk-services.%s/validate-android-signature - https://%sinapps.%s/api/v - https://%smonitorsdk.%s/api/remote-debug/v2.0?app_id= - https://%sadrevenue.%s/api/v2/generic/v6.13.1/android?app_id=	com/appsflyer/internal/AF1eSDK.java
https://%smonitorsdk.%s/remote-debug/exception-manager	com/appsflyer/internal/AFc1cSDK.java
https://%simpimpression.%s	com/appsflyer/share/CrossPromotionHelper.java
- https://%sonelink.%s/shortlink-sdk/v2 - https://%sars.%s/api/v2/android/validate_subscription?app_id= - https://%sars.%s/api/v2/android/validate_subscription_v2?app_id= - https://%sviap.%s/api/v1/android/validate_purchase?app_id= - https://%sgcdsdk.%s/install_data/v5.0/ - https://%sviap.%s/api/v1/android/validate_purchase_v2?app_id=	com/appsflyer/internal/AFe1wSDK.java
https://%sregister.%s/api/v	com/appsflyer/internal/AFg1oSDK.java
https://%sapp.%s	com/appsflyer/internal/AFj1vSDK.java
https://appv.ivoji.id/index.html	com/ivoji/commonlibrary/ui/WelcomeActivity.java
https://%sdlsdk.%s/v1.0/android/	com/appsflyer/internal/AFf1nSDK.java
- https://gdpr.adjust.world - https://app.adjust.com - https://gdpr.eu.adjust.com - https://%svalidate.%s/api/v - https://%scdn-%ssettings.%s/android/v1/%s/settings - https://subscription.adjust.com - https://%ssdk-services.%s/validate-android-signature - https://github.com/adjust/android_sdk#can-it-trigger-an-event-at-application-launch - https://%sars.%s/api/v2/android/validate_subscription_v2?app_id= - https://%sviap.%s/api/v1/android/validate_purchase?app_id= - https://.facebook.com - https://%sgcdsdk.%s/install_data/v5.0/ - https://subscription.adjust.world - www.facebook.com 3.0.9.1 - https://gdpr.tr.adjust.com - https://gdpr.us.adjust.com - https://facebook.com/device?user_code=%1\$s&qr=1 - https://app.us.adjust.com - https://subscription.eu.adjust.com - https://%sonelink.%s/shortlink-sdk/v2 - https://aps-webhandler.appsflyer.com/api/trigger - https://%sconversions.%s/api/v	

- https://appv.ivoji.id/index.html - https://app.adjust.world - https://%/s/%s/%s - https://goo.gl/naoooi - http://goo.gl/8rd3yj - https://%sdlSDK.%s/v1.0/android/ - https://graph.%s - https://app-measurement.com/a - https://%smonitorsdk.%s/api/remote-debug/v2.0?app_id= - https://www.linkedin.com - https://%sinapps.%s/api/v - https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps - www.google.com - https://%smonitorsdk.%s/remote-debug/exception-manager - https://app.adjust.cn - https://accounts.google.com - https://firebase.google.com/support/guides/disable-analytics - https://%sadrevenue.%s/api/v2/generic/v6.13.1/android?app_id= - https://www.facebook.com - https://app.adjust.net.in - https://%sattr.%s/api/v - https://%slaunches.%s/api/v - https://app.eu.adjust.com - https://%sadrevenue.%s/api/v2/log/adimpression/v6.13.1/android?app_id= - https://firebase.google.com/support/privacy/init-options - https://%scdn-%stestsettings.%s/android/v1/%s/settings - https://twitter.com - https://%sregister.%s/api/v - https://gdpr.adjust.net.in - https://facebook.com - http://goo.gl/nafqkq - https://google.com/search? - https://accounts.google.com/o/oauth2/revoke?token= - https://login.live.com - https://gdpr.adjust.com - https://app.tr.adjust.com - https://www.googletagmanager.com - https://ivoji-001.firebaseio.com - https://www.paypal.com - https://%simpression.%s - https://goo.gl/j1swqy - https://login.yahoo.com - https://%sars.%s/api/v2/android/validate_subscription?app_id= - https://subscription.adjust.net.in - https://%sapp.%s - https://graph-video.%s - https://www.google.com - https://subscription.adjust.com - https://subscription.us.adjust.com - https://plus.google.com/ - https://%savian.%s/api/v1/android/validate_purchase_v2?app_id= - http://hospitame/?	自研引擎-S
https://aip.baidubce.com/public2.0/license/face-api/app/querydevicelicense	lib/arm64-v8a/libbd_unifylicense.so

🔹 Firebase 配置安全检测

标题	严重程度	描述信息

第三方 SDK 组件分析

SDK名称	开发者	描述信息
百度人脸识别	Baidu	人脸离线识别 SDK，包含人脸采集、活体检测、人脸对比/识别、人脸库管理等能力，并全部离线化、本地化。
C++ 共享库	Android	在 Android 应用中运行原生代码。
Paddle Lite	Baidu	Paddle Lite 是一个高性能、轻量级、灵活性强且易于扩展的深度学习推理框架，致力于支持包括移动端、嵌入式以及边缘端在内的多种硬件平台。当前 Paddle Lite 不仅在百度内部业务中得到全面应用，也成功支持了众多外部用户和企业的生产任务。
AndroidUtilCode	Blankj	AndroidUtilCode 是一个强大易用的安卓工具类库，它合理地封装了安卓开发中常用的函数，具有完善的 Demo 和单元测试，利用其封装好的 APIs 可以大大提高开发效率。
Google Sign-In	Google	提供使用 Google 登录的 API。
Google Play Service	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图、Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
File Provider	Android	FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 代替 file:///Uri 以促进安全分享与应用程序关联的文件。
Jetpack App Startup	Google	App Startup 库提供了一种直接、高效的方法在应用程序启动时初始化组件。库开发人员 and 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。
Firebase	Google	Firebase 提供实时数据库、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。
Google Analytics	Google	提供各种 API，可帮助您收集、配置和报告用户与您的在线内容进行互动的数据。
Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的分析数据。

第三方追踪器检测

名称	类别	网址
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

敏感凭证泄露检测

可能的密钥
"google_api_key" : "AlzaSyChDHiKoVrX6sfjumpifRiRqdpS8T9J_Xo"
"ACCOUNT_KIT_CLIENT_TOKEN" : "e811ba78598e782564e388e4bfd0f5f3"
"google_crash_reporting_api_key" : "AlzaSyChDHiKoVrX6sfjumpifRiRqdpS8T9J_Xo"
"firebase_database_url" : "https://ivoji-001.firebaseio.com"
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F

► Google Play 应用市场信息

标题: IVOJI: Pinjaman tanpa ribet

评分: 4.380608 **安装:** 1,000,000+ **价格:** 0 **Android版本支持:** 分类: 财务 **Play Store URL:** [id.ivoji](#)

开发者信息: PT Finansia Aira Teknologi, PT+Finansia+Aira+Teknologi, CitraGrand Ciburur CBD Fraser Park FR01 No.1 - 17424, <https://www.ivoji.id>, customer@ivoji.id,

发布日期: None **隐私政策:** [Privacy link](#)

关于此应用:

IVOJI 已在金融服务管理局 (OJK) 注册并受其监管。IVOJI 已由 OJK 正式注册并运营，许可证号：KEP-73/D/05/2021。我们提出了一个数字金融科技平台，将贷款人（贷款人）和借款人（贷款接受人）在合法、安全、透明的范围内聚集在一起，从而创建融资和借贷交易，使贷款人能够从管理的贷款收益中获得利润。由借款人。贷款产品：可获得的每日贷款含服务费为 IDR. 500,000 卢比 - 400 万。该贷款适用于需要短期贷款的雇员和小型企业。贷款规格：- 贷款金额：IDR 500,000 - IDR 4,000,000 - 货币贷款期限：91-180 天 - 低利息（最高）：每年 36% - 预付费用：无（根据批准的贷款金额全额收到资金）贷款模拟：例如，对于期限为 91 天、金额为 2,000,000 印尼盾的贷款，收取的费用如下：- 月利率：36%/12 = 3% - 每月利息：IDR 2,000,000*3% = IDR 60,000 - 每月付款总额 = IDR 2,000,000/3 + IDR 60,000 = IDR 726,667 - 总利息：2,000,000 印尼盾 * (36%/365) * 91 天 = 180,000 印尼盾 - 总退货费用：IDR 2,000,000 + IDR 180,000 = IDR 2,180,000 如何在 IVOJI 注册成为资助者：1. 下载 IVOJI 应用程序并选择作为资助者 2. 正确、完整地填写您的个人资料。• 年龄 21-65 岁 • 提交所需文件，例如带照片的身份证、NPWP 和自拍照 • 以您自己的名义拥有一个个人储蓄账户 • 拥有个人电子邮件 • 确保您填写的数据符合实际情况。拿起我们验证团队的电话验证您填写的数据 3. 作为网贷出资人等待审批结果 4. 选择您想要融资的借款人的资料 5. 根据您想要注资的名义金额进行转账 6. 签署协议 如何在 IVOJI 注册成为借款人：1. 下载 IVOJI 应用程序并选择作为借款人 2. 正确、完整地填写您的个人资料。• 年龄 21-60 岁 • 印度尼西亚公民 (WNI) • 提交身份证照片、自拍照片等所需文件 • 每月最低收入 3,000,000 印尼盾 • 以您自己的名义拥有一个个人储蓄账户 • 拥有个人电子邮件 • 确保您填写的数据符合实际情况。拿起我们验证团队的电话验证您填写的数据 3. 等待网贷审核审核结果 4. 资金将发送至您的账户 IVOJI 管理的所有产品均已根据 POJK 77 No.1 调整为符合印度尼西亚有关金融科技贷款的 OJK 法规。2016 年 我们的官方服务 电子邮件: customer@ivoji.id 服务时间: 周一至周五, 09:00 - 17:00 地址: PT. 艾拉金融技术公司 Jl. H. R. Rasuna Said No.B12 Floor 16 Block E2, RT.6/RW.7, Kuningan, Karet Kuningan, Setiabudi District, South Jakarta City, Special Capital Region of Jakarta 12940

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，深入扫描软件中潜在的漏洞和安全隐患。

© 2025 南明离火 - 移动安全分析平台自动生成