南明离火

移动应用检测平台

ANDROID 静态分析报告

Finanzas Ágiles • v1.0.03

分析日期: 2025-08-27 15:47:42

应用概览

文件名称:	com.finanzasagiles.credito.apk
文件大小:	7.28MB
应用名称:	Finanzas Ágiles
软件包名:	com.finanzasagiles.credito
主活动:	com.bmc.dash.dinerodash.MainActivity
版本号:	1.0.03
最小SDK:	21
目标SDK:	34
加固信息:	未加壳
开发框架:	Flutter
应用程序安全分数:	57/100 (中风险)
跟踪器检测:	4/432
杀软检测:	经检测，该文件安全
MD5:	ff1b532d4ad082e7219b718cd60f2f5f
SHA1:	fdd0f4347e1573[illegible]a295f780ef69be311d[illegible]2a5f
SHA256:	deffdfc86134c35577d82f08004d11976b8869a093e3a3cf029417acb76fcc2

分析结果严重性分布

高危	中危	信息	安全	关注
1	16	1	3	0

四大组件导出状态统计

Activity组件：3个，其中export的有： 0个
Service组件：10个，其中export的有： 1个
Receiver组件：4个，其中export的有： 2个
Provider组件：4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: 2024-12-11 12:06:38+00:00
有效期至: 2054-12-11 12:06:38+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0x8fc213fbfa61c7c0dfe2e719937d8e184f7f2f11
哈希算法: sha256
证书MD5: ab91913fb9d786fe03b53dc36a4eda4a
证书SHA1: 2d412ea40ba6e88271cabb41577941dac9c6e26b
证书SHA256: 4b302a15525b5e01c364b8f338ab930fef637d5599bbcb888f700e39586e2ab8
证书SHA512:
54baf7897f73dfff41386133b99f8dd78d8aaf0da5ed78d3b686b1e0348d90bd9fe3a8d27fec311bb29a70236ce66237169c7d22952f4a[illegible]e3d653a520ba0ff0a

公钥算法: rsa
密钥长度: 4096
指纹: f0594cbbd06303cf64bc1f96ff4f4beefd671aae881ab0de3e45d85ffa42ccfb
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
android.permission.READ_SMS	危险	读取短信	允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。
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粗略的经纬度信息，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.READ_PHONE_STATE	危险	读取手机状态和标识	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
android.permission.READ_CALENDAR	危险	读取日历活动	允许应用程序读取您手机上存储的所有日历活动。恶意应用程序可借此将您的日历活动发送给其他人。
android.permission.WRITE_CALENDAR	危险	添加或修改日历活动以及向邀请对象发送电子邮件	允许应用程序添加或更改日历中的活动，这可能会向邀请对象发送电子邮件。恶意应用程序可能会借此清除或修改您的日历活动，或者向邀请对象发送电子邮件。
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_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.READ_BASIC_PHONE_STATE	普通	允许对基本电话状态信息进行只读访问	允许只读访问具有非危险权限的手机状态，包括蜂窝网络类型、软件版本等信息。
android.permission.ACCESS_WIFI_STATE	普通	查看Wi-Fi状态	允许应用程序查看有关Wi-Fi状态的信息。
android.permission.ACCESS_ADSERVICES_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.samsung.android.mapsagent.permission.READ_APP_INFO	未知	未知权限	来自 android 引用的未知权限。
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	未知权限	来自 android 引用的未知权限。
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。
android.permission.ACCESS_ADSERVICES_AD_ID	普通	允许应用访问设备的广告 ID。	此 ID 是 Google 广告服务提供的唯一、用户可重置的标识符，允许应用出于广告目的跟踪用户行为，同时维护用户隐私。
com.finanzasagiles.credito.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
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。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.bmc.dash.dinerodash.MainActivity	Schemes: finanzasagiles://,

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: **4** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。
2	Broadcast Receiver (com.dinerodash.permission_util.SmsReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.gms.auth.api.phone.permission.SEND [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。
3	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	警告	检测到 Service 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。
4	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: **1** | 警告: **10** | 信息: **1** | 安全: **2** | 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	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限
3	应用程序可以读取/写入外部存储器，任何应用程序都可以读取写入外部存储器的数据	警告	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
5	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
6	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
7	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限
8	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
9	文件可能包含硬编码的敏感信息，如用户名、密码、密钥等	警告	CWE: CWE-312: 明文存储敏感信息 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
10	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员：解锁高级权限
11	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	警告	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

12	此应用程序可能会请求root（超级用户）权限	警告	CWE: CWE-250: 以不必要的权限执行 OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
13	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
14	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

应用行为分析

编号	行为	标签	文件
00162	创建 InetSocketAddress 对象并连接到它	socket	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	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
00096	连接到 URL 并设置请求方法	命令 网络	升级会员：解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限
00146	获取网络运营商名称和 IMSI	电话服务 信息收集	升级会员：解锁高级权限
00078	获取网络运营商名称	信息收集 电话服务	升级会员：解锁高级权限
00171	将网络运算符与字符串进行比较	网络	升级会员：解锁高级权限
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限
00005	获取文件的绝对路径并将其放入 JSON 对象	文件	升级会员：解锁高级权限

00117	获取 IMSI 和网络运营商名称	电话服务 信息收集	升级会员：解锁高级权限
00137	获取设备的最后已知位置	位置 信息收集	升级会员：解锁高级权限
00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员：解锁高级权限
00066	查询ICCID号码	信息收集	升级会员：解锁高级权限
00067	查询IMSI号码	信息收集	升级会员：解锁高级权限
00076	获取当前WiFi信息并放入JSON中	信息收集 WiFi	升级会员：解锁高级权限
00083	查询IMEI号	信息收集 电话服务	升级会员：解锁高级权限
00113	获取位置并将其放入 JSON	信息收集 位置	升级会员：解锁高级权限
00014	将文件读入流并将其放入 JSON 对象中	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
00051	通过setData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
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00161	对可访问性节点信息执行可访问性服务操作	无障碍服务	升级会员：解锁高级权限
00173	获取 AccessibilityNodeInfo 屏幕中的边界并执行操作	无障碍服务	升级会员：解锁高级权限
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00192	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00011	从 URI 查询数据（SMS、CALLLOGS）	短信 通话记录 信息收集	升级会员：解锁高级权限
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00134	获取当前WiFi IP地址	WiFi 信息收集	升级会员：解锁高级权限
00001	初始化位图对象并将数据（例如JPEG）压缩为位图对象	相机	升级会员：解锁高级权限
00183	获取当前相机参数并更改设置	相机	升级会员：解锁高级权限
00065	获取SIM卡提供商的国家代码	信息收集	升级会员：解锁高级权限

00153	通过 HTTP 发送二进制数据	http	升级会员：解锁高级权限
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00094	连接到 URL 并从中读取数据	命令 网络	升级会员：解锁高级权限
00062	查询WiFi信息和WiFi Mac地址	WiFi 信息收集	升级会员：解锁高级权限
00034	查询当前数据网络类型	信息收集 网络	升级会员：解锁高级权限
00082	获取当前WiFi MAC地址	信息收集 WiFi	升级会员：解锁高级权限
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00202	打电话	控制	升级会员：解锁高级权限
00203	将电话号码放入意图中	控制	升级会员：解锁高级权限
00030	通过给定的 URL 连接到远程服务器	网络	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	7/30	android.permission.READ_SMS android.permission.ACCESS_COARSE_LOCATION android.permission.READ_PHONE_STATE android.permission.READ_CALENDAR android.permission.WRITE_CALENDAR 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 android.permission.ACCESS_WIFI_STATE 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-ssettings.s	安全	否	No Geolocation information available.
sgcdsdk.s	安全	否	No Geolocation information available.

svalidate-and-log.s	安全	否	No Geolocation information available.
pagead2.googlesyndication.com	安全	是	**IP地址:** 180.163.151.38 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.230416 **经度:** 121.473701 **查看:** 高德地图
simpression.s	安全	否	No Geolocation information available.
sconversions.s	安全	否	No Geolocation information available.
sapp.s	安全	否	No Geolocation information available.
slaunches.s	安全	否	No Geolocation information available.
sinapps.s	安全	否	No Geolocation information available.
scdn-stestsettings.s	安全	否	No Geolocation information available.
spia.s	安全	否	No Geolocation information available.
sdlsdk.s	安全	否	No Geolocation information available.
ssdk-services.s	安全	否	No Geolocation information available.
svalidate.s	安全	否	No Geolocation information available.
sregister.s	安全	否	No Geolocation information available.
smonitorsdk.s	安全	否	No Geolocation information available.
sattr.s	安全	否	No Geolocation information available.
sonelink.s	安全	否	No Geolocation information available.
firebase-settings.crashlytics.com	安全	是	**IP地址:** 180.163.150.34 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.230416 **经度:** 121.473701 **查看:** 高德地图
sadrevenue.s	安全	否	No Geolocation information available.
privacy-sandbox.appsflyersdk.com	安全	否	**IP地址:** 18.155.202.48 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	q3/b.java
• https://%spia.%s/api/v1.0/pia-android-event?app_id=	com/appsflyer/internal/AFf1jSDK.java
• https://accounts.google.com/o/oauth2/revoke?token=	v3/f.java
• https://%sconversions.%s/api/v • https://privacy-sandbox.appsflyersdk.com/api/trigger • https://%ssdk-services.%s/validate-android-signature • https://%smonitorsdk.%s/api/remote-debug/v2.0?app_id= • https://%svalidate.%s/api/v • https://%sinapps.%s/api/v • https://%slaunches.%s/api/v • https://%sattr.%s/api/v • https://%sdlsdk.%s/v1.0/android/ • https://%sadrevenue.%s/api/v2/generic/v6.15.2/android?app_id=	com/appsflyer/internal/AFj1jSDK.java
• https://%sapp.%s	com/appsflyer/internal/AFj1iSDK.java
• https://%sregister.%s/api/v	com/appsflyer/internal/AFg1jSDK.java
• https://firebase.google.com/docs/crashlytics/get-started?platform=android#add-plugin	o5/c0.java
• https://%scdn-%stestsettings.%s/android/v1/%s/settings • https://%scdn-%ssettings.%s/android/v1/%s/settings	com/appsflyer/internal/AFe1iSDK.java
• javascript:findwebrtcinfo	com/datavisorobfus/h.java
• https://%simpression.%s	com/appsflyer/share/CrossPromotionHelper.java
• https://%s/%s/%s	k6/c.java
• https://%smonitorsdk.%s/remote-debug/exception-manager	com/appsflyer/internal/AFd1aSDK.java
• https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings	w5/g.java
• https://github.com/baseflow/flutter-permission-handler/issues	m2/t.java
• https://%svalidate.%s/api/v1.0/android/validateandlog?app_id= • https://%sgcdsdk.%s/install_data/v5.0/ • https://%sonelink.%s/shortlink-sdk/v2	com/appsflyer/internal/AFe1qSDK.java

Firebase 配置安全检测

标题	严重程度	描述信息

Firebase远程配置已禁用	安全	Firebase远程配置URL （ https://firebaseremoteconfig.googleapis.com/v1/projects/1006300130426/namespaces/firebase:fetch?key=AIzaSyAA3uL5D0O6XK0t02QpNENrWwLfh_-d4VQ ） 已禁用。响应内容如下所示：
		{
		"state": "NO_TEMPLATE"
		}

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。
神策分析 SDK	神策	神策分析，是针对企业级客户推出的深度用户行为分析产品，支持私有化部署，客户端、服务器、业务数据、第三方数据的全端采集和建模，驱动营销渠道效果评估、用户精细化运营改进、产品功能及用户体验优化、老板看板辅助管理决策、产品个性化推荐改造、用户标签体系构建等应用场景。作为 PaaS 平台支持二次开发，可通过 BI、大数据平台、CRM、ERP 等内部 IT 系统，构建用户数据体系，让用户从数据发挥深远的价值。
File Provider	Android	FileProvider 是 ContentProvider 的特殊子类，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。
Firebase	Google	Firebase 提供了分析、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。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
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
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Google Crashlytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Sensors Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/248

敏感凭证泄露检测

可能的密钥
"google_api_key" : "AIzaSyAA3uL5D0O6XK0t02QpNENrWwLfh_-d4VQ"
"google_app_id" : "1:1006300130426:android:0061aaaecaec15509d5fc3"
"google_crash_reporting_api_key" : "AIzaSyAA3uL5D0O6XK0t02QpNENrWwLfh_-d4VQ"
MJCR3nbjtc8ARKt9HOAI/AZAzrHiEyhubQ==
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
KZGR3Uffq88OW6tuEewC9j5V3A==
470fa2b4ae81cd56ecbcda9735803434cec591fa
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
H6ik7UfoqtAwYIZxE9A68jVW8J/oAjw=
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
dI2H2mzZqo8OQIQxI/oZ8itF3Lf7XC57dQ==
MJCR3nbjtc8ARKt/AP825zhTxLPuFzw=
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075EAC46D8C667EAE7212

Google Play 应用市场信息

标题: Finanzas Ágiles-Crédito Fácil

评分: 4.8568087 **安装:** 100,000+ **价格:** 0 **Android版本支持:** **分类:** 财务 **Play Store URL:** com.finanzasagiles.credito

开发者信息: Finanzas Ágiles, Finanzas+%C3%81giles, None, https://www.finanzasagiles.com, help@finanzasagiles.com,

发布日期: None **隐私政策:** Privacy link

关于此应用:

Agile Finance 是一款全新的在线个人贷款应用程序，专为墨西哥市场设计，旨在为用户提供便捷、透明、快速且灵活的贷款服务。只需在线提交您的国民身份证件（INE）照片和其他个人信息，即可快速申请贷款，并可根据您的需求调整贷款金额和期限。无论您是用于个人消费、教育支出还是家庭需求，Agile Finance 都能为您提供最合适的贷款方案。 主要特点 快速申请：只需几个步骤即可完成申请。系统智能审批，快速提供结果。 透明利率：利率、还款日期、分期金额等信息清晰显示，确保无任何隐藏费用。 灵活的付款方式：我们提供多种付款方式，您可以选择提前还款或延期付款，以满足您的需求。 安全保障：我们使用先进的加密技术保护您的所有个人信息和交易，防止数据泄露和欺诈。 便捷的付款提醒：我们实施贴心的付款提醒，不会给用户带来不便。 产品信息 灵活的贷款金额：您可以选择 4,000 墨西哥比索至 20,000 墨西哥比索之间的贷款金额，最高限额为 20,000 墨西哥比索。 灵活的还款期限：您可以选择 91 至 180 天之间的还款期限，最长期限为 180 天。 低利率和透明的费用：我们提供极具竞争力的利率，最低日利率为 0.01%，最低年利率 (APR) 为 3.6%，最高日利率为 0.1%，最高年利率 (APR) 为 36%。 此信息将根据您的个人信息和信用状况确定。贷款金额、期限和利率以最终批准为准。 如果您向 Finanzas Ágiles 申请一笔 20,000 墨西哥比索的贷款，期限为 180 天（6 个月），日利率为 0.1%（年利率 36%），则您需要支付以下费用： 每日利息：20,000 美元 * 0.1% = 20 美元 每月应付利息：20,000 美元 * 0.1% * 180 天 / 30 天 = 600 美元 应付利息总额：20,000 美元 * 0.1% * 180 天 = 3,600 美元 每月本金支付额：20,000 美元 / 6 个月 = 3,333 美元 每月还款总额：3,333 美元 + 600 美元 = 3,933 美元 应付总额：20,000 美元 + 3,600 美元 = 23,600 美元 以上数字仅供参考仅限。最终金额取决于审批结果和具体条件。 申请要求 年满18周岁，并持有有效的官方身份证件（INE）。 拥有稳定的收入来源或良好的信用记录。 无需拥有不良信用记录。 隐私政策 使用Agile Finance，我们深知保护您的个人信息至关重要。我们致力于确保您的数据安全，并严格遵守适用的法律法规。我们收集的信息将通过https://www.finanzasagiles.com上传到Agile Finance服务器，并将加密存储，以确保数据

免责声明及风险提示:

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。