



ANDROID 静态分析报告



Empower MX v1.29.4.340

分析日期: 2025-08-27 11:21:07

i应用概览

文件名称:	finance.empower.mx.apk
文件大小:	30.65MB
应用名称:	Empower MX
软件包名:	finance.empower.mx
主活动:	finance.empower.android.app.LaunchActivity
版本号:	1.29.4.340
最小SDK:	24
目标SDK:	35
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	52/100 (中风险)
跟踪器检测:	5/432
杀软检测:	经检测，该文件安全
MD5:	aefafb53d696822abdbfc59a781ff54b
SHA1:	b0ee0a137e701376c32e07889ff865c9e2c94d8a9
SHA256:	f4f62c407571a2ce86d544830ad4d83da4f3517c2e6d4efc7ec25a5b9859380d

分析结果严重性分布

高危	中危	信息	安全	关注
3	19	3	3	0

四大组件导出状态统计

Activity组件: 20个，其中export的有: 3个
Service组件: 10个，其中export的有: 0个
Receiver组件: 4个，其中export的有: 2个
Provider组件: 8个，其中export的有: 0个

应用签名证书信息

APK已签名
v1 签名: False
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: 2022-08-23 00:22:47+00:00
有效期至: 2052-08-23 00:22:47+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0x28613418788d3d135780a8efbd8380a9659339e3
哈希算法: sha256
证书MD5: aec9bfc0ec60800f68e8c790f038c8f3
证书SHA1: b009e1311f5186e40363a77bbcd1a54db6759bd1
证书SHA256: 95a8d77b92bec3cb369728576d31b9b6d5eb41ab2b9e28ca51c61bffc6d176b
证书SHA512:
a045e136dd8f82c3fed2eb249fa1745295f1d47644a8f6a8eb32ad55492302a5d617cc52d33266aea5890c5e0477ce6372e180f93ce74fe2619ebf6bc35e511a

公钥算法: rsa
密钥长度: 4096
指纹: b5bbcd7e7a3b0cb93ac6b0cf24bd7352ba37f9e4ce60ab2ec86e8e01f221240dc
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.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_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_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。
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。
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_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.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.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。
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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.USE_BIOMETRIC	普通	使用生物识别	允许应用使用设备支持的生物识别方式。
android.permission.USE_FINGERPRINT	普通	允许使用指纹	此常量在 API 级别 28 中已弃用。应用程序应改为请求USE_BIOMETRIC
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。
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_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。
android.permission.ACCESS_AD_SERVICES_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.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。
finance.empower.mx.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
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.android.vending.CHECK_LICENSE	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
finance.empower.android.app.DeepLinkLaunchActivity	Schemes: http://, https://, empower-mx://, Hosts: open.empowerapp.mx,
com.stripe.android.link.LinkRedirectHandlerActivity	Schemes: link-popup://, Hosts: complete, Paths: /finance.empower.mx,
com.stripe.android.payments.StripeBrowserProxyReturnActivity	Schemes: stripesdk://, Hosts: payment_return_url, Paths: /finance.empower.mx,

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: 0 | 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: 6 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	Activity (finance.empower.android.app.DeepLinkLaunchActivity) 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	Activity 设置了 TaskAffinity 属性 (finance.empower.android.app.loan.repayment.stripe.LoanAddDebitCardInfoView)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
3	Activity (com.stripe.android.link.LinkRedirectHandlerActivity) 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。
4	Activity (com.stripe.android.payments.StripeBrowserProxyReturnActivity) 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。
5	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.c2dm.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。

6	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: 2 | 警告: 11 | 信息: 3 | 安全: 3 | 屏蔽: 0

序号	问题	等级	参考标准	文件位置
1	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
2	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
3	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
4	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
5	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
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	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MST G-CODE-2	升级会员：解锁高级权限
8	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: MST G-STORAGE-2	升级会员：解锁高级权限
9	此应用程序具有防止窃听攻击的功能	安全	OWASP MASVS: MST G-PLATFORM-9	升级会员：解锁高级权限
10	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MST G-PLATFORM-7	升级会员：解锁高级权限
11	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: MST G-NETWORK-4	升级会员：解锁高级权限
12	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: MST G-STORAGE-2	升级会员：解锁高级权限
13	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
14	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: MST G-RESILIENCE-1	升级会员：解锁高级权限
15	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MST G-CRYPTO-3	升级会员：解锁高级权限

16	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MST G-STORAGE-10	升级会员：解锁高级权限
17	应用程序可以写入应用程序目录。敏感信息应加密	信息	CWE: CWE-276: 默认权限不正确 OWASP MASVS: MST G-STORAGE-14	升级会员：解锁高级权限
18	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: MST G-PLATFORM-7	升级会员：解锁高级权限
19	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: MST G-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
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
00013	读取文件并将其放入流中	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
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
00012	读取数据并放入缓冲流	文件	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
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
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
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

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
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
00091	从广播中检索数据	信息收集	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
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
00075	获取设备的位置	信息收集 位置	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
00115	获取设备的最后已知位置	信息收集 位置	升级会员：解锁高级权限
00162	创建 InetAddress 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
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
00195	设置录制文件的输出路径	录制音视频 文件	升级会员：解锁高级权限
00199	停止录音并释放录音资源	录制音视频	升级会员：解锁高级权限
00198	初始化录音机并开始录音	录制音视频	升级会员：解锁高级权限
00194	设置音源（MIC）和录制文件格式	录制音视频	升级会员：解锁高级权限
00197	设置音频编码器并初始化录音机	录制音视频	升级会员：解锁高级权限
00007	Use absolute path of directory for the output media file path	文件	升级会员：解锁高级权限
00196	设置录制文件格式和输出路径	录制音视频 文件	升级会员：解锁高级权限
00114	创建到代理地址的安全套接字连接	网络 命令	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
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
00132	查询ISO国家代码	电话服务 信息收集	升级会员：解锁高级权限
00025	监视要执行的一般操作	反射	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.ACCESS_COARSE_LOCATION android.permission.READ_SMS android.permission.WRITE_CALENDAR android.permission.READ_PHONE_STATE android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.WAKE_LOCK
其它常用权限	6/46	android.permission.INTERNET android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_NETWORK_STATE com.google.android.gms.permission.AD_ID com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE com.google.android.c2dm.permission.RECEIVE

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.
clientsdk.launchdarkly.com	安全	否	IP地址: 151.101.129.55 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

clientstream.launchdarkly.com	安全	否	IP地址: 151.101.129.55 国家: 美国 地区: 华盛顿 城市: 西雅图 纬度: 47.604309 经度: -122.329842 查看: Google 地图
twitter.com	安全	否	IP地址: 54.187.175.68 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
sgcdsdk.s	安全	否	No Geolocation information available.
q.stripe.com	安全	否	IP地址: 54.187.159.182 国家: 美国 地区: 美国俄勒冈州 城市: 董事会成员 纬度: 45.839855 经度: -119.7005834 查看: Google 地图
withpersona.com	安全	否	IP地址: 162.159.141.40 国家: 美国 地区: 美国加利福尼亚州 城市: 旧金山 纬度: 37.718128 经度: -122.4343849 查看: Google 地图
pagead2.google syndication.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
docs.stripe.com	安全	是	IP地址: 221.228.32.13 国家: 中国 地区: 中国江苏 城市: 南京 纬度: 32.060255 经度: 118.796877 查看: 高德地图
api.stripe.com	安全	否	IP地址: 54.149.153.72 国家: 美国 地区: 美国俄勒冈州 城市: 董事会成员 纬度: 45.839855 经度: -119.7005834 查看: Google 地图
simpresion.s	安全	否	No Geolocation information available.

checkout.link.com	安全	否	IP地址: 18.155.202.13 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
sconversions.s	安全	否	No Geolocation information available.
hooks.stripe.com	安全	否	IP地址: 54.187.175.68 国家: 美国 地区: 美国俄勒冈州 城市: 董事会成员 纬度: 45.850855 经度: -119.7001834 查看: Google 地图
link.co	安全	否	IP地址: 54.187.175.68 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
goo.gle	安全	否	IP地址: 54.187.175.68 国家: 美国 地区: 纽约 城市: 纽约市 纬度: 40.713192 经度: -74.006065 查看: Google 地图
sapp.s	安全	否	No Geolocation information available.
merchant-ui-api.stripe.com	安全	否	IP地址: 54.187.175.68 国家: None 地区: 俄勒冈 城市: 波特兰 纬度: 45.523460 经度: -122.676468 查看: Google 地图
slaunches.s	安全	否	No Geolocation information available.
api.empowerapp.mx	安全	否	IP地址: 52.152.58.88 国家: 美国 地区: 得克萨斯州 城市: 圣安东尼奥 纬度: 29.424120 经度: -98.493729 查看: Google 地图
sinapps.s	安全	否	No Geolocation information available.

m.stripe.com	安全	否	IP地址: 52.152.58.88 国家: 美国 地区: 俄勒冈 城市: 波特兰 纬度: 45.523460 经度: -122.676468 查看: Google 地图
empower.withpersona.com	安全	否	IP地址: 172.66.1.36 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
scdn-stestsettings.s	安全	否	No Geolocation information available.
sars.s	安全	否	No Geolocation information available.
spia.s	安全	否	No Geolocation information available.
link.com	安全	否	IP地址: 54.789.200.54 国家: 美国 地区: 俄勒冈 城市: 波特兰 纬度: 45.523460 经度: -122.676468 查看: Google 地图
errors.stripe.com	安全	否	IP地址: 198.202.176.161 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
empowerapp.mx	安全	否	IP地址: 75.2.60.5 国家: 美国 地区: 华盛顿 城市: 西雅图 纬度: 47.604309 经度: -122.329842 查看: Google 地图
docs.withpersona.com	安全	否	IP地址: 64.239.109.1 国家: 美国 地区: 加利福尼亚 城市: 核桃 纬度: 34.020519 经度: -117.865532 查看: Google 地图

firebase-settings.crashlytics.com	安全	是	IP地址: 180.163.150.162 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
sdlSDK.s	安全	否	No Geolocation information available.
support.stripe.com	安全	否	IP地址: 63.33.88.220 国家: 美国 地区: 纽约 城市: 纽约市 纬度: 40.7128192 经度: -74.006015 查看: Google 地图
youtrack.jetbrains.com	安全	否	IP地址: 63.33.88.220 国家: 爱尔兰 地区: 爱尔兰伦斯特 城市: 都柏林 纬度: 53.3465322 经度: -6.3423318 查看: Google 地图
ssdk-services.s	安全	否	No Geolocation information available.
svalidate.s	安全	否	No Geolocation information available.
mobile.launchdarkly.com	安全	否	IP地址: 52.20.210.136 国家: 美国 地区: 弗吉尼亚州 城市: 阿什本 纬度: 39.039474 经度: -77.491806 查看: Google 地图
sregister.s	安全	否	No Geolocation information available.
stripe.com	安全	否	IP地址: 35.167.54.49 国家: 美国 地区: 俄勒冈 城市: 波特兰 纬度: 45.523460 经度: -122.676468 查看: Google 地图
inquiry-fallback.withpersona.com	安全	否	IP地址: 34.111.150.223 国家: 美国 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
smonitorsdk.s	安全	否	No Geolocation information available.
sattr.s	安全	否	No Geolocation information available.

privacy-sandbox.appsflyersdk.com	安全	否	IP地址: 18.155.202.106 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
sonelink.s	安全	否	No Geolocation information available.
svalidate-and-log.s	安全	否	No Geolocation information available.
sadrevenue.s	安全	否	No Geolocation information available.
sviap.s	安全	否	No Geolocation information available.
webrtc-consumer.withpersona.com	安全	否	IP地址: 172.66.1.36 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://static.ada.support/embed2.js	自研引擎-A
https://play.google.com/store/apps/details?id=finance.empower.mx&hl=es-mx&gl=mx	ec/S.java
https://play.google.com/store/apps/details?id=	Ed/d.java
https://youtrack.jetbrains.com/issue/kt-5980	Gf/G.java
https://%sregister.%s/api/v	com/appsflyer/internal/AFg1eSDK.java
- https://%sconversions.%s/api/v - https://privacy-sandbox.appsflyersdk.com/api/logger - https://%ssdk-services.%s/validate-android-signature - https://%smmonitorsdk.%s/api/remote-debug/v2.0?app_id= - https://%svalidate.%s/api/v - https://%sadrevenue.%s/api/v2/genetic/v6.16.0/android?app_id= - https://%smapps.%s/api/v - https://%slaunches.%s/api/v - https://%sattr.%s/api/v - https://%sdlSDK.%s/v1.0/android/	com/appsflyer/internal/AFj1bSDK.java
https://%smmonitorsdk.%s/remote-debug/exception-manager	com/appsflyer/internal/AFe1xSDK.java
- https://api.stripe.com/edge-internal/ - https://api.stripe.com/v1/ - https://merchant-ui-api.stripe.com/elements/	com/stripe/android/networking/a.java

- https://hooks.stripe.com/three_d_secure/authenticate - https://hooks.stripe.com/redirect/complete/ - https://hooks.stripe.com/3d_secure/complete/ - https://hooks.stripe.com/3d_secure_2/hosted/complete	com/stripe/android/view/C3997r0.java
https://checkout.link.com/#	o8/PopupPayload.java
https://firebase.google.com/docs/crashlytics/get-started?platform=android#add-plugin	M5/C2242z.java
https://goo.gle/compose-feedback	S0/AbstractC7295o.java
https://m.stripe.com/6	b9/f.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	m3/b.java
https://firebase.google.com/docs/crashlytics/get-started?platform=android#add-plugin	M5/C072fz.java
- https://hooks.stripe.com/three_d_secure/authenticate - https://hooks.stripe.com/redirect/complete/ - https://hooks.stripe.com/3d_secure/complete/ - https://hooks.stripe.com/3d_secure_2/hosted/complete	com/stripe/android/view/S186r0.java
- https://inquiry-fallback.withpersona.com/part - https://inquiry-fallback.withpersona.com/template - https://inquiry-fallback.withpersona.com/session	com/withpersona/sdk2/inquiry/internal/fallbackmode/FallbackModeService.java
https://api.stripe.com/v1/	l9/b.java
https://errors.stripe.com/api/	Q9/a.java
- https://link.co/privacy - https://link.co/terms	Q8/g.java
- https://clientsdk.launchdarkly.com - https://mobile.launchdarkly.com - https://clientstream.launchdarkly.com	com/launchdarkly/sdk/android/h0.java
https://console.firebase.google.com/	q6/b.java
https://emv3ds/challenge	com/stripe/android/stripe3ds2/views/e.java
https://emv3ds/challenge	com/stripe/android/stripe3ds2/views/f.java
http://10.0.2.2:8969/stream	io/sentry/SpotlightIntegration.java
https://%simpression.%s	com/appsflyer/share/CrossPromotionHelper.java
- https://%sars.%s/api/v2/android/validate_subscription_v2?app_id= - https://%swiap.%s/api/v1/android/validate_purchase?app_id= - https://%svalidate-and-log.%s/api/v1.0/android/validateandlog?app_id= - https://%sconelink.%s/shortlink-sdk/v2 - https://%swiap.%s/api/v1/android/validate_purchase_v2?app_id= - https://%sars.%s/api/v2/android/validate_subscription?app_id= - https://%sgcdsdk.%s/install_data/v5.0/	com/appsflyer/internal/AFe1sSDK.java

- https://withpersona.com - https://webrtc-consumer.withpersona.com	com/withpersona/sdk2/inquiry/internal/f.java
- https://withpersona.com - https://webrtc-consumer.withpersona.com	com/withpersona/sdk2/inquiry/internal/g.java
- https://stripe.com/docs/api/setup_intents/object#setup_intent_object-status - https://stripe.com/docs/api/payment_intents/object#payment_intent_object-confirmation_method - https://stripe.com/docs/api/payment_intents/object#payment_intent_object-status	F9/k.java
https://empower.withpersona.com	finance/empower/android/app/onboarding/idverification/PersonalIdVerificationActivity.java
https://stripe.com/docs/keys	r8/C7183a.java
https://stripe.com/docs/keys	r8/C2877a.java
https://stripe.com/es-mx/legal	finance/empower/android/app/loan/repayment/stripe/LoanAddDebitCardInfoView.java
https://%/s/%s/%s	I6/c.java
- https://%scdn-%stestsettings.%s/android/v1/%s/settings - https://%scdn-%ssettings.%s/android/v1/%s/settings	com/appsflyer/internal/AFe1eSDK.java
- https://docs.stripe.com/payments/external-payment-methods?platform=android#available-external-payment-methods - https://support.stripe.com/questions/activate-a-new-payment-method	F9/d.java
https://stripe.com/es-mx/legal	finance/empower/android/app/profile/legal/j.java
- https://docs.google.com/gview?embedded=true&url= - https://docs.google.com	finance/empower/android/app/web/b.java
https://%sapp.%s	com/appsflyer/internal/AFk1wSDK.java
https://docs.withpersona.com/docs/mobile-sdks-v1	Ra/m.java
https://twitter.com/stripestatus	com/stripe/android/core/exception/APIConnectionException.java
https://api.empowerapp.mx	kc/C5734b.java
https://api.empowerapp.mx	kc/C1875b.java
https://empowerapp.mx/	de/a.java
https://%s pia.%s/api/v1.0/pia-android-event?app_id=	com/appsflyer/internal/AFf1fSDK.java
https://plus.google.com/	T3/n0.java
https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings	U5/g.java
https://q.stripe.com	x8/C3040b.java

https://q.stripe.com	x8/C7839b.java
- https://link.com/terms/ach-authorization - https://stripe.com/ach-payments/authorization	y9/i.java
https://stripe.com/legal/bacs-direct-debit-guarantee	自研引擎-S

🔥 Firebase 配置安全检测

标题	严重程度	描述信息
		Firebase远程配置URL（https://firebaseremoteconfig.googleapis.com/v1/projects/294954864360/namespace/firebase:fetch?key=A1zaSyABmJ5cxtOwqeg5pQ4jLJdYBDofijwVWI）已启用。请确保这些配置不包含敏感信息。响应内容如下所示： <pre>{ "entries": { "address_validation_prompt_enabled": "true", "app_review_prompt_enabled": "true", "bank_statement_experiment_enabled": "false", "bank_statement_inferred_end_date": "true", "bank_statement_instruction_banks": "{}", "bank_statement_instructions_enabled": "false", "bank_statement_on_home_screen": "true", "bank_statement_oom_fix": "false", "bank_statement_password_support": "false", "bank_statement_password_support_v2": "true", "bank_statement_skip_flow_enabled": "false", "belvo_access_route_disabled": "false", "change_phone_number_on_login_enabled": "false", "connected_accounts_enabled": "true", "display_already_existing_user_screen": "true", "email_confirmation_modal_enabled": "true", "debit_card_show_justification": "false", "duv_2_enabled": "true", "enable_state_verification_for_statements_upload": "false", "fix_anr_encryption_enabled": "true", "home_feed_feature_radar_enabled": "true", "home_feed_modal_frequency_prompt": "{ \"fix_penny_auth\": 86400000, \"fix_delivery_account_id\": 86400000, \"fix_bank_statement\": 86400000, \"credit_report\": 86400000, \"address_validation\": 86400000, \"fix_debit_card\": 86400000 }", "improve_referral_code_capture": "true", "landing_screen_show_new": "true", "launch_darkly_extra_logs_enabled": "true", "loan_due_date_on_calendar_enabled": "false", "loan_experiment_fixed_percent_fee": "true", "loan_experiment_high_amount_modal_enabled": "true", "loan_experiment_preselect_middle_enabled": "true", "loan_experiment_variable_percent_fee": "false", "loan_interest_every_day_enabled": "false", "loan_max_amount": "5000", "loan_multi_offers_enabled": "false", "loan_multi_offers_fix_enabled": "true", "loan_multi_repay_date_enabled": "true", "loan_repayment_show_oxxo": "false", "loan_tile_show_fees": "true", "messaging_communication_channel": "1",</pre>

Firebase远程配置已启用	警告	<pre>"number_of_bank_statements_required": "3", "onboarding_address_enabled": "false", "onboarding_address_validation_details": "{ \"enabled\": false, \"neighbourhood_required\": false, \"municipality_required\": false }", "onboarding_cic_critical_action_enabled": "false", "onboarding_cic_enabled": "true", "onboarding_curp_validation_enabled": "true", "onboarding_free_form_kyc_enabled": "true", "onboarding_id_verification_info_view_enabled": "false", "onboarding_id_verification_show_customer_support": "true", "onboarding_name_as_password_input_enabled": "true", "onboarding_references_details": "{ \"enabled\": true, \"mandatory_references_required\": 2, \"mandatory_disclosure\": false }", "onboarding_reset_phone_number_enabled": "true", "onboarding_show_welcome_call_screen": "false", "onboarding_submit_appsflyer_details_enabled": "true", "optimized_sms_parser_enabled": "true", "penny_auth_belvo_retries": "{ \"belvo_retries\": { \"bancoazteca_mx_retail\": 0, \"bancoppel_mx_retail\": 0, \"banorte_mx_retail\": 0, \"banregio_mx_retail\": 7, \"bancomer_mx_retail\": 0, \"banamex_mx_retail\": 7, \"hsbc_mx_retail\": 7, \"inbursa_mx_retail\": 7, \"liverpool_mx_retail\": 7, \"santander_mx_retail\": 0, \"scotiabank_mx_retail\": 7 } }", "penny_auth_enabled": "true", "permission_read_calendar_enabled": "true", "permission_read_phone_state_enabled": "true", "permission_read_sms_early_ask": "false", "permission_read_sms_enabled": "true", "permissions_details": "{ \"access_fine_location\": { \"title\": { \"us\": \"Get your location\", \"mx\": \"Conectar tu ubicación\" }, \"description\": { \"us\": \"We use the location permission for fraud prevention and enhanced security.\", \"mx\": \"Usamos tu ubicación para prevenir intentos de fraude y reforzar la seguridad de la app.\" }, \"enabled\": true, \"mandatory\": false }, \"get_accounts\": { \"enabled\": false, \"mandatory\": false }, \"read_contacts\": { \"title\": { \"us\": \"Contacts\", \"mx\": \"Tu lista de contactos\" }, \"description\": { \"us\": \"We use this information exclusively as input for our credit model, we do not share this information and we will never contact anyone on your contact list.\", \"mx\": \"Utilizamos esta información exclusivamente para nuestros modelos de crédito o no compartimos esta información con nadie más y nunca nos pondremos en contacto con ninguno de tus contactos.\" }, \"enabled\": false, \"mandatory\": false }, \"read_sms\": { \"title\": { \"us\": \"SMS\", \"mx\": \"Mensajes de texto\" }, \"description\": { \"us\": \"We use this information exclusively as input for our credit model and this also helps our models validate your identity, we will never share the content of your messages.\", \"mx\": \"Utilizamos esta información exclusivamente para nuestros modelos de crédito y también nos ayuda a validar tu identidad, nunca compartiremos el contenido de tus mensajes con nadie.\" }, \"enabled\": true, \"mandatory\": false }, \"read_calendar\": { \"title\": { \"us\": \"Calendar\", \"mx\": \"Calendario\" }, \"description\": { \"us\": \"We use this information exclusively as input for our credit model, we do not share this information.\", \"mx\": \"Solamente utilizamos esta información como un parámetro en nuestro modelo de crédito, nadie más tendrá acceso a esta información.\" }, \"enabled\": true, \"mandatory\": false }, \"read_phone_state\": { \"title\": { \"us\": \"Phone state\", \"mx\": \"Estado del teléfono\" }, \"description\": { \"us\": \"This ensures that the cell phone number is active, and that it is linked to the device you are using to open the account.\", \"mx\": \"Esto nos ayuda a validar que el número de celular esté activo y que esté vinculado al dispositivo que se está utilizando para abrir la cuenta.\" }, \"enabled\": true, \"mandatory\": false } }", "permissions_enabled": "true", "permissions_home_feed_prompt_enabled": "true", "permissions_home_feed_prompt_frequency_days": "1", "permissions_minimal_word_count": "5", "permissions_network_details_as_json": "false", "permissions_to_server": "true", "permissions_underwriting_list_apps": "true", "persona_template_new_sex_enabled": "true",</pre>
----------------------------	---------------	---

		<pre>"prompt_active_loan_users": "false", "prompt_to_play_store": "false", "reference_accepts_sms": "true", "referral_amount": "100", "referral_code_fix": "true", "referral_from_loan_enroll_enabled": "true", "referral_landing_screen_cheer_lady_enabled": "false", "referral_landing_screen_full_text_enabled": "true", "referrals_enabled": "false", "referrals_enabled_dynamic_link": "true", "sentry_cut_launch_darkly_logs_enabled": "true", "sentry_disable_span_traces": "true", "sentry_enable_user_interaction": "false", "show_other_banks_tile_enabled": "true", "skip_belvo_link_account_enabled": "true", "spei_instruction_banks": "{ \"banks\": [\"bancomer_mx_retail\", \"bancoazteca_mx_retail\"] }", "stripe_continue_on_intent_answered": "false", "stripe_continue_on_intent_launched": "true", "stripe_intents_enabled": "true", "support_communication_channel": "{ \"options\": { \"whatsapp_url\": \"https://wa.me/525539718338\", \"zendesk_number\": \"525531718338\" }", "support_custom_modal_details": "{ \"title_en\": \"Important\", \"details_en\": \"We are currently experiencing intermittent issues with the SPEI network, so we are unable to send or receive transfers. If you're having trouble accepting or paying your loan, please try again in a few hours. Thank you for your patience and understanding.\", \"title_es\": \"Aviso Importante\", \"details_es\": \"En este momento estamos experimentando retrasos con el envío y recepción de pagos. No es necesario que lo reportes.\" }", "support_custom_modal_enabled": "false", "survey_questions_enabled": "true", "tech_retrofits_config": "{ \"live_config\": { \"fetch_live_config\": false }, \"bank_statements\": { \"submit_bank_statement\": false, \"submit_most_recent\": false, \"dates_required\": false, \"fetch_bank_statement\": false }, \"user\": { \"fetch_user\": false, \"delete_user\": false, \"email_add\": false, \"email_verify\": false, \"call_initiate\": false, \"user_details\": false, \"user_meta\": false, \"user_references\": false, \"questionnaire_data\": false, \"user_attribution\": false }, \"penny\": { \"submit_clabe\": false }, \"loan_agreement\": { \"fetch_existing_loan_agreements\": false, \"fetch_existing_loan_agreement_document\": false, \"fetch_existing_loan_agreement_document_with_new_repay_date\": false, \"fetch_loan_offer_agreement_document\": false, \"accept_loan_offer_agreement\": false } }", "upload_statements_enabled": "true", "version_management": "{ \"android\": { \"min_required_version\": 167, \"min_recommended_version\": 16 } }", "whatsapp_copy_to_prefill_enabled": "false", "whatsapp_prefill_on_button_tapped_enabled": "false" }, "state": "UPDATE", "templateVersion": "395" }</pre>
--	--	---

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。

✉ 邮箱地址敏感信息提取

EMAIL	源码文件
support@stripe.com	b9/f.java
email@me.co	r8/b.java
support@stripe.com	com/stripe/android/core/exception/URLConnectionException.java
support@stripe.com	x8/C104f.java
support@stripe.com	x8/C7843f.java
support@stripe.com david.hernandez@ahorros.com	自研引擎-S

🕸 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
Segment	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/62
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

🔑 敏感凭证泄露检测

可能的密钥

"com.google.firebase.crashlytics.mapping_file_id" : "e934273bf8144dfaa773c11004c4072a"
"debit_card_auth_start" : "Comenzar"
"google_api_key" : "AIzaSyABmJ5cxtOwqeg5pQ4jLjxUyBD9fijwVWI"
"google_app_id" : "1:294954864360:android:cc0a228385a0c01e98435d"
"google_crash_reporting_api_key" : "AIzaSyABmJ5cxtOwqeg5pQ4jLjxUyBD9fijwVWI"
"onboarding_cic_authorize" : "Autorizar"
Vn3kj4pUblROi2S+QfRRL9nhsaO2uoHQg6+dpEtxdTE=
b6abbffd-e952-4eea-8d7e-06346c7f55f9
115792089210356248762697446949407573530086143415290314195533631308867097853951
b9ce7bac-72ca-432f-9039-a556ea907149
cc2affa3-4e7c-4e62-b414-e2969c2d31b0
EC0786B4-3970-4D38-9633-0D413860F903
78fe4ac1-a1fd-490c-a252-ceee31b540d4
55066263022277343669578718895168534326250603453777594175500187360389116729240
645ff40a-27e4-4e18-84c9-bc6444a25187
832571096148902998554675128952010817928785304886134559470920590248050319938419224438643760392947333078086511627871
2dcbc461-579e-4b70-9a82-4ef8be212734
6cd2d33a-193d-4209-9c74-f96c161f284e
b35c289d-ace7-456d-9998-d7bb56f31f86
4b47af9b-9408-4271-94f7-01928d412d56
0d0c46c9-0e0c-4f51-ba34-f737f085e126
0bf30166-75b8-46e0-9962-6ab03c2ac6c8
4170fde1-2dc4ffa-8335-e6ed593e394d
fe14e61b-7df7-4eb5-b4e1-0eb0111235595
d8eafb1d-bee7-4af7-8c63-d80787550827
3f1f26d7-8a09-41e7-a598-b5674cf87a8e
6a647b05-574d-488c-998d-16617fbe4fe7
9e8e61f1-b13a-45fe-8571-a6a15bb04323
e15a6438-a14e-4b55-9675-4c162bc96464

50599905-613f-4141-a805-e31d7a0f147f
a3652498-9140-4d30-8d0b-b530fe433ccd
2661740802050217063228768716723360960729859168756973147706671368418802944996427808491545080627771902352094241225065558662157113545570916814161637315895999846
0e8b47f2-2acf-4407-a224-a9d84d46b373
e2bbdf63-bdb0-469a-b7b6-51c7e6058357
19ed5791-f48a-43f6-ac19-e1dc04904230
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861600873112319
c345a9be-64ed-4a12-9c22-ca78c6af136e
19af9ecd-92df-4d07-81f2-f1d009f19ed8
6520a466-560a-482d-9caa-91b1f3cdac9c
36134250956749795798585127919587881956611106672985015071877198253568414405109
c77159b9-11de-4b13-a583-46fb2e322889
09fe9d10-31f5-4737-896b-2431f1609d9d
66bd202c-073e-4a6d-9ba9-1d12d011b876
d54c6760-1f55-4c60-ab0d-9413837c03bf
911d008f-96d1-4351-a1eb-40f627fa3f68
39402006196394479212279040100143613805079739270465446667946905279627059399113263569398956308152294913554433653942643
838e86ad-06b3-4cfb-a8b1-656f0a7c0170
93f5b2fb-87e6-44cd-be1c-f174fdce7355
769ff0d6-1608-4203-b374-d3c5949d6946
b6abbffd-e629-431b-a1fb-3d53f9ec020a
5d73069e-e1a0-4746-b784-9fb7c22a544d
702e86c7-0b5e-4d46-9e5a-62090a16b3a5
4a2b33f2-bd34-432b-a05b-278131c65b3c
12E4C725-4902-4898-8DA5-0880800587ED
152d5a3d-3e7e-4f8b-b38a-089c404d7652
308b90b5-4071-4208-ae6c-8355813c34d5
cb6871e5-f201-43fd-a6d9-e39424d4d135

32670510020758816978083085130507043184471273380659243275938904335757337482424
df62bab8-2710-4a7e-8f96-72dc431d9968
030f0e10-946e-40de-ac83-e27a9ef21513
ed1179cc-7710-411e-b387-ea802287e24e
a68e7c9f-ef16-4884-8efd-8a06ba57e59a
35b4ec40-ec93-4bbb-a910-89d75020657e
115792089210356248762697446949407573529996955224135760342422259061068512044369
7B5E452C-7EDD-41A2-93D8-DA92DFFA019D
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
ca4802c4-55b2-4ec0-9e92-48d2df02adcd
9E1231C3-FB82-4DF2-A452-90A7E760B4F3
115792089237316195423570985008687907852837564279074904382605163141518161494237
d0b6c5a1-c86f-44bd-b101-22d9619e26f2
3D26B985-3A79-40A4-A148-A50D24297091
0e0b293e-8e04-4d46-a0b1-21d124fbb458
fe867f36-6e64-4801-92bf-1d4534a616be
49c21ada-72be-4003-8b75-6bfd7e5f424b
lajXe5K+w8s2lyhXbTG5ttXrQasrnijKUcYb/8ttf2a
8YyN590KODDFDRwzv9J1yICU3aVqknpq
188cfdbb-9fbf-42f6-ae08-8ee521b2a10
09C11E13-F327-43E1-BE95-B372005D642C
c1a3dbe2-a0e8-4e6c-8fa0-1b3036f0f34d
e6266a4b-72c-4a44-87e7-151bd7d2c930
484395612939064517590525859527974202762949526041747995844080717082404635286
109384903807373427451112390766805569936207598951683748994586394495953116150735016013708737573759623248592132296706313309438452531591012912142327488478985984
491216D9-EB15-41A0-961D-57B7EDA23B73
6616b23f-4a60-4ae3-958c-3d7eb7c397b0
6436909b-a4c0-4219-ac9b-60c7e4d26f58

27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575
f94f255b-7e66-4cb5-9650-ba6d88cbbdcc
74a5d153-38d7-4363-bb1e-6e38f55486ba
6520f1ba-bd48-492b-8fa1-663bb77fb24b
b-c0196d28-2f00-4226-a080-b4cb787ec888
001cd5b2-aa61-462b-b61a-cd3b75a60a2b
0cc05d1c-f673-4ca9-8182-8cee1d445ee1
26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786350872476732087
76DAAD29-F63D-4241-ABAC-04047BEF3C8A
3f0020cc-3358-4962-ad3f-4d57c3d11139
3b677a0f-0fe9-4226-a4f1-4f34d3edd43c
A4A6F880-5323-4747-844C-F7F29E03F42A
115792089210356248762697446949407573530086143415290314195533631308867007853948
6B2A3AA8-8EC6-4F96-A87B-B450A8275487
17d8bb0e-6d9f-4551-a632-baa72c5df975
542f288a-86e0-4bcc-83de-5459f10a3fa6
5D081812-99CD-41A6-AEF3-75269AFCE91C
a1330fa2-bc8f-4b31-95d1-3bb14f87acb3
fd4817e2-3c73-4531-93f7-ac76b2262f56
39402006196394479212279040100143613805079739270465146667948293404245721771496870329047266088258938001861606973112316
470fa2b4ae81cd56ecb0fa9735803434cec591fa
ade2a4c3-53ed-417a-a1e4-3df3a63b1614
51Ky39eX23msroucKaMQt8S9N2qCwspnqL/PwrEaa6EWacbDrUg8sYHQpxl1HqSfuSFqANBAHmJUC5FTYrq1PVzF00Z2f9s7DT
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148
115792089237316195423570985008687907853269984665640564039457584007908834671663
5acd74ab-48ee-42bc-a159-770ad39d9b0d
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
a259f727-7c52-424d-abdf-706f352ab129

7c9f1bae-1d10-4deb-bd30-200e13a3a58d
09393388-40ee-4486-ac87-11b6b16c55f7
0484477d-cff9-47d7-adf4-ec2e119f6390
890d22c9-7ef6-47eb-ae79-2f456b1373f1
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
70654039-6d78-4b23-851b-0ba8042515c7
32f83308-896b-47cd-a04c-88a5ac3e7486
96740bec-9117-42d2-b6e2-1e45850543b1
2ec0805e-0e79-4a5e-96a6-f36abb0b54ba
3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289128522585666729196580810124344277578376784
474f5612-9624-46a9-9240-5d1dfa4ba12b
58f17278-e6ab-4e96-86ba-a585954ba004
7c998a04-9942-4219-b1bc-0927ca17d5a5
c5137200-9b05-4850-891f-1d72eb47d6de
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52E04138EAAA08901
0f73a834-d44b-492c-a8bd-a097a91ab753
cbef559f-8da6-48f4-9328-110a701f79fe
bec0bd72-4e0a-412c-9d67-b488d3d867ac
0d0f5aab-8b2a-4380-96d5-66fbb361b52c
31ed9f15-ee09-419e-ae2b-31c48d506a59
4550f139-501d-498a-8012-c9a101779e81
4f93dee7-01d7-4865-b16c-d87a738ea010
dfc68ba4-8796-4545-9bba-77490163832c
E7EE317C-6201-49F2-AC72-43BAAB82F1F4
FFE391E0EA186D0734FD001E4E70E3224B7309D48E2075BAC46D8C667EAE7212
686479766013060914981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999710643812571028291115057151
2858292b-eb51-491b-9366-21d22b8edd9e
7537c499-a06d-45ec-af87-72e637961f61

e59c5cb4-2926-4aa4-8bc8-bac474dbb408
089115F1-1C50-4364-AB4D-F1497E4D6C3B
8703bf81-f361-4507-a0f0-0095c4bae6d0
9ae49e5e-246c-4ca5-9c1b-b5483b95223d
e0b25bdc-39af-40fc-9168-1d9df9195665
12278850-bc66-4a07-a609-96d26e25060e
e0e6389b-34fd-4c5b-bb4b-b7a81f1bf086
8d6f3355-6a7a-4cb2-a9ae-681d1daeea89
0a6f9dee-85d9-49e0-b7ed-96447a9f277c
851fc4e4-243f-4131-a219-fbf02b891664
1ea9b0a0-3d47-4f34-8bdf-773bd53424c2
B9497879-F3A4-403B-B211-8295BA8A8900
6D94E9D4-E50F-41A5-9045-969959225D63
f512a125-dbbb-46cc-88bb-a75493e08cd2
cbf92f5f-6589-49b9-baf9-4741c43dedef
56A58F10-C629-4DDE-A110-461FFB8C4698
dcb428fea25c40e7b99f81ae5981ee6a
30f20ae7-e357-45a1-a265-7067db9c7e83
5de5e29f-ab38-4c06-b859-1d8600372841

► Google Play 应用市场信息

标题: Empower: préstamo en minutos

评分: 4.8754287 安装: 1,000,000+ 价格: 0 Android 版本支持: 分类: 财务 Play Store URL: [finance.empower.mx](https://play.google.com/store/apps/details?id=com.finance.empower)

开发者信息: Fin Finance, 4977150831260126756, None, <http://empowerapp.mx/>, ayuda@empowerapp.mx,

发布日期: None 隐私政策: [Privacy link](#)

关于此应用:

几分钟内即可获得高达 5,000 美元的贷款 - 在您最需要的时候提供。直接在您的帐户中收到款项，佣金清晰，无需任何细则。赋能如何运作？ 1.下载 Empower 2. 创建帐户。您只需要您的手机和INE 3. 完成一份简短的申请。告诉我们一些关于您自己的信息，并帮助我们核实您的收入* 4. 在几分钟内获得您的贷款报价。您的手机接受并在您的帐户中收到款项 5.别担心。 Empower 将在约定日期自动收取您的贷款，但您始终可以选择进行 SPEI 转账并支付您的信用额度 *Empower 使用开放银行技术来验证您的收入 00 无障碍 透明且固定的佣金 00 立即 填写您的申请，如果您的请求获得批准，您的帐户将在几分钟内收到款项 00方便 直接在申请中请求积分 24/7 00轻松支付 不用担心并避免滞纳金。 Empower 将在约定日期自动收取您的贷款，但您始终可以选择进行 SPEI 转账并支付您的信用额度 00持续访问 当您需要新贷款时，返回申请表。我们随时为您提供帮助 Empower 贷款示例： 接受 1,000 美元贷款并选择 61 天期限的用户，在付款日期必须一次性付款总计 1,174.00 美元。付款包括 1,000 美元的贷款本金、150 美元的固定费用（贷款本金的 15%）以及 16% 的增值税。不含增值税的贷款 CAT 为 128%。除上述费用外，我们不收取任何利息。总付款明细： \$1,000（贷款本金）+ \$150（\$1,000 * 15% 固定费用）+ \$24（\$150 费用 * 16% 增值税）= \$1,174.00 条款和费用 贷款金额： \$150 - \$5,000 固定发起费： 贷款金额的 15% 加增值税 固定年违

约利率: 360% 加增值税 滞纳金: 贷款金额的10%加增值税 最短付款期限: 61 天 最长付款期限: 61 天 信息平均 CAT: 1137% (不含增值税) * *CAT 平均 1137% (不含增值税)。仅供参考和比较之用。CAT 计算日期: 2023 年 12 月。Empower 绝不会在上述基础上收取额外的佣金或利息 谁可以获得 Empower 贷款: 00 年满 18 岁的墨西哥公民 00 您需要您的手机号码和有效的 INE 或 IFE 00 您名下的银行账户 隐私政策 您向我们提供的信息将专门用于验证您的身份并批准您的信贷申请。请在此处查看我们的隐私政策, 详细了解 Empower 如何收集、使用和共享您的个人和/或敏感数据: <https://empowerapp.mx/legal/aviso-de-privacidad> 在进行任何交易之前, 请务必阅读并理解条款和条件以及信贷协议。产品改进 我们始终致力于改进我们的产品和客户体验。如果我们提供的产品与此处描述的产品不同, 请随时与我们联系。 接触 电子邮件: help@empower.me 网站: empowerapp.mx 电话: +52 55 9302 0604

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