南明离火
移动应用检测平台

ANDROID 静态分析报告

ChatUp AI - v1.0.28

分析日期: 2025-07-07 08:53:18

应用概览

文件名称:	ChatUp AI-(Mod)-by天辰-1.0.28.apk
文件大小:	14.7MB
应用名称:	ChatUp AI
软件包名:	org.chatupai
主活动:	org.chatupai.ui.beforeLogin.activities.splashActivity.SplashActivity
版本号:	1.0.28
最小SDK:	24
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:	52/100 (中风险)
跟踪器检测:	7/432
杀软检测:	AI评估：安全
MD5:	f65f33b4793e10787716b89b0433f7ce
SHA1:	3e2dc8b4fe20263dd74c97135c0eb2636b5dd8d
SHA256:	b2b367eb09f858eb398b09a26ab82d59171ec994c4288b755e366d240baf820

分析结果严重性分布

高危	中危	信息	安全	关注
2	11	2	2	0

四大组件导出状态统计

Activity组件：20个，其中export的有： 1个
Service组件：6个，其中export的有： 0个
Receiver组件：5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: False
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
证书MD5: e89b158e4bcf988ebd09eb83f5378e87
证书SHA1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
证书SHA512:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640[illegible]053abfea3039772721[illegible]04d89b7711292a4569

公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75
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.VIBRATE	普通	控制振动器	允许应用程序控制振动器，用于消息通知振动功能。
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.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.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。
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.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。

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.android.vending.BILLING	普通	应用程序具有应用内购买	允许应用程序从 Google Play 进行应用内购买。
org.chatupai.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: fbconnect:// Hosts: cct.org.chatupai,

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: **4** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
2	Broadcast Receiver (com.adjust.sdk.AdjustReferrerReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.INSTALL_PACKAGES [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	Activity (com.facebook.CustomTabActivity) 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	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: **6** | 信息: **2** | 安全: **1** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
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	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
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	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	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	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	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
9	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
10	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: MSTG-STORAGE-10	升级会员：解锁高级权限

应用行为分析

编号	行为	标签	文件
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
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00123	连接到远程服务器后将响应保存为 JSON	网络 命令	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
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
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
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

00108	从给定的 URL 读取输入流	网络 命令	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
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
00046	方法反射	反射	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
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
00189	获取短信内容	短信	升级会员：解锁高级权限
00188	获取短信地址	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
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00200	从联系人列表中查询数据	信息收集 联系人	升级会员：解锁高级权限
00201	从通话记录中查询数据	信息收集 通话记录	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
00163	创建新的 Socket 并连接到它	socket	升级会员：解锁高级权限
00162	创建 InetSocketAddress 对象并连接到它	socket	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	3/30	android.permission.VIBRATE android.permission.RECORD_AUDIO android.permission.WAKE_LOCK
其它常用权限	5/46	android.permission.INTERNET android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_NETWORK_STATE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE com.google.android.gms.permission.AD_ID

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
configs-cdn.adapty.io	安全	否	**IP地址:** 52.52.144.126 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
api.chatupai.org	安全	否	**IP地址:** 52.52.144.126 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774919 **经度:** -122.419418 **查看:** Google 地图
fallback.adapty.io	安全	否	**IP地址:** 172.67.43.89 **国家:** 加拿大 **地区:** 安大略 **城市:** 多伦多 **纬度:** 43.6532 **经度:** -79.3832 **查看:** Google 地图
api.adapty.io	安全	否	**IP地址:** 104.26.12.205 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
api.ipify.org	安全	否	**IP地址:** 52.52.144.126 **国家:** 美国 **地区:** 加利福尼亚 **城市:** l(BÎûÂ84þm £ Ê ¼NBýÁ¾94äl F© à qHBué A<4¾k }á f 6Bõ,Â=4{w / ï >B **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
dashboard.chatupai.org	安全	否	**IP地址:** 52.52.144.126 **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
• http://play.google.com/store/apps/details?id=	org/chatupai/utils/UtilsKt.java
• https://dashboard.chatupai.org/terms-of-service • https://dashboard.chatupai.org/api/ • https://dashboard.chatupai.org/privacy-policy • https://api.chatupai.org/api/v1/	org/chatupai/utils/AppConstants.java
• https://api.adapty.io/api/v1/sdk/	com/adapty/internal/data/cloud/Request.java
• https://configs-cdn.adapty.io/api/v1/sdk/ • https://api.ipify.org?format=json • https://fallback.adapty.io/api/v1/sdk/	com/adapty/internal/data/cloud/RequestFactory.java
• 8.1.2.3 • 8.1.2.2 • 8.1.2.1	io/grpc/okhttp/OkHttpServerTransport.java
• 127.0.0.1	io/grpc/okhttp/OkHttpClientTransport.java
• http://undefined/	org/jsoup/helper/HttpConnection.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/356677136002/namespaces/firebase:fetch?key=AIzaSyCn57ufTAkG2kDX6pcT5UGW1q9AZLoHyIQ ）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 Play Billing	Google	Google Play 结算服务可让您在 Android 上销售数字内容。本文档介绍了 Google Play 结算服务解决方案的基本构建基块。要决定如何实现特定的 Google Play 结算服务解决方案，您必须了解这些构建基块。
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 Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
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。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).

邮箱地址敏感信息提取

EMAIL	源码文件
chatup@emeraldlabs.ai	自研引擎-S

第三方追踪器检测

名称	类别	网址
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Places		https://reports.exodus-privacy.eu.org/trackers/69
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

敏感凭证泄露检测

可能的密钥
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"

"facebook_app_id" : "448842584732204"
"facebook_client_token" : "80be2447522a84a6b554693caca54dd9"
"google_api_key" : "AIzaSyCn57ufTAkG2kDX6pcT5UGW1q9AZLoHyIQ"
"google_app_id" : "1:356677136002:android:ede995feca5ae885c60e9b"
"google_crash_reporting_api_key" : "AIzaSyCn57ufTAkG2kDX6pcT5UGW1q9AZLoHyIQ"
5e8f16062ea3cd2c4a0d547876baa6f38cabf625
cc2751449a350f668590264ed76692694a80308a
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
9b8f518b086098de3d77736f9458a3d2f6f95a37

Google Play 应用市场信息

标题: ChatUp AI - Chat Bot Assistant

评分: 4.4 **安装:** 1,000+ **价格:** 0 **Android**版本支持: **分类:** 效率 **Play Store URL:** org.chatupai

开发者信息: Emerald Labs LLC, Emerald+Labs+LLC, None, https://chatupai.org/, chatup@emeraldlabs.ai,

发布日期: 2024年7月14日 **隐私政策:** Privacy link

关于此应用:

通过 ChatUp 获取日常任务的灵感！ ChatUp 由高级语言模型 ChatGPT 和 GPT-4o 提供支持。我们的应用程序保持了人性化的感觉，交互很流畅。无论您是在朝九晚五的生活中寻求帮助，还是在寻找灵感作家，ChatUp 都是适合您的人工智能应用程序。 输入您的请求或从数十个提示中进行选择，我们的人工智能将经历提出解决方案和响应的客观过程。使用我们强大的古董 AI 聊天机器人开始生成创意内容并升级您的写作。 人工智能写作助手 ChatUp 为每一个可以想象到的想法提供动力，不要犹豫，针对您的想法和问题提出后续问题。这个人工智能可以做到这一切。 电子邮件生成器 生成您需要的任何电子邮件，您可以针对任何情况制作原创的、引人注目的专业电子邮件。 语法和拼写检查器 ChatUp 可以快速纠正文本中的语法、拼写和标点错误。 文本到图像生成 ChatUp 可以将任何新颖的想法变成任何风格的新颖且鼓舞人心的图像。 网页分析器 使用我们的浏览聊天功能浏览网络寻找答案，它将立即编译链接和来源。您还可以使用我们的链接和询问功能来了解您提供的任何链接。 YouTube专业版 这个应用程序将立即转录大多数 YouTube 视频。只需粘贴链接，它就会总结、重写、翻译它，或回答您有关其内容的所有问题。 文档大师 从您的文件中上传任何文档并以您想要的方式对其进行分析。 语音转文字功能 ChatUp 可以轻松回答您的问题，只需点击语音功能，它就会写下您所说的内容。 文字转语音选项 没有时间阅读？只需使用我们的收听功能并收听文本即可。 专业订阅 - 您可以订阅以无限制地访问某些应用程序功能 - 订阅将按照所选订阅计划的费率自动计费 立即下载 ChatUp，充分利用人工智能革命！ 服务条款： https://dashboard.chatupai.org/terms-of-service 隐私政策： https://dashboard.chatupai.org/privacy-policy

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。