



MoGua

Calculator 2.0.APK 分析报告



APP名称:

Calculator

包名:	com.tzt_entry
域名线索:	7条
URL线索:	8条
邮箱线索:	0条
分析日期:	2025年7月16日
分析平台:	摸瓜APK反编译平台

文件名: 23Admin 2025.apk
文件大小: 47.86MB
MD5值: 8fb7b0477c65d5fe2a4c811b1c103159
SHA1值: 16e1ca995f5cb203526128aa5938683be8c30afd
SHA256值: ed26343e050378365056ffa4fe2b993a6f6af7b4ca2aa8943927c8d84fcad70b

i APP 信息

App名称: Calculator
包名: com.tzt_entry
主活动Activity: com.tzt_entry.MainActivity
安卓版本名称: 2.0
安卓版本: 2

🔍 域名线索

域名	服务器信息
ns.adobe.com	没有服务器地理信息.
plus.google.com	IP: 66.220.147.11 所属国家: United States of America 地区: California 城市: Menlo Park 纬度: 37.436935 经度: -122.193604
www.facebook.com	IP: 205.186.152.122 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806

pinterest.com	IP: 157.240.10.36 所属国家: United States of America 地区: California 城市: Menlo Park 纬度: 37.436935 经度: -122.193604
wap.kbipay.com	IP: 159.138.1.199 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
twitter.com	IP: 162.159.140.229 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
codepush.appcenter.ms	没有服务器地理信息.

URL线索

URL信息	Url所在文件
https://wap.kbipay.com/apk/sdk/download/	com/kbipay/payment/KBZPay.java
https://codepush.appcenter.ms/	com/microsoft/codepush/react/CodePush.java
http://ns.adobe.com/xfdf/	com/tom_roush/pdfbox/pdmodel/fdf/FDFDocument.java
https://www.facebook.com/sharer/sharer.php?u=	cl/json/social/FacebookPagesManagerShare.java

https://www.facebook.com/sharer/sharer.php?u=	cl/json/social/FacebookShare.java
https://plus.google.com/share?url=	cl/json/social/GooglePlusShare.java
https://pinterest.com/pin/create/button/?url=	cl/json/social/PinterestShare.java
https://twitter.com/intent/tweet?text=	cl/json/social/TwitterShare.java

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=95, ST=yangon, L=yangon, O=studio_zeroone, OU=studio_zeroone, CN=zeroone
签名算法: rsassa_pkcs1v15
有效期自: 2018-10-19 08:20:58+00:00
有效期至: 2046-03-06 08:20:58+00:00
发行人: C=95, ST=yangon, L=yangon, O=studio_zeroone, OU=studio_zeroone, CN=zeroone
序列号: 0x7a9c5793
哈希算法: sha256
md5值: 80f97160fcfe68e322fcc933e48b7661
sha1值: 0d3cc0107f0ac79013a79f4ffac306b2f552c58a
sha256值: dd9c0ca417caad372216fa97051f769087807a7543c5cc4c1447a204b7b575c6
sha512值: b12153828d689f731fcdf6fe7224c25db6777575c750ad337609b92457263645887964a78a207ca92943a228e05cfcc6a36457defe4a6f0f9af233741a3ee4c1
公钥算法: rsa
密钥长度: 2048
指纹: 6a5128c903e6fe13c00adcd41edf9081e47106be9acb5a0b00976cb2e016685d

硬编码敏感信息

可能的敏感信息
"CodePushDeploymentKey" : "3mnVB49khmH4IAwFHvgk28AeirzRbNZ6_KbGd2"
"com_facebook_device_auth_instructions" : "Visit facebook.com/device and enter the code shown above."
"google_api_key" : "AlzaSyAA9i0G-qIVKPHAPP5wbwbeijUej9_AQpk"
"google_crash_reporting_api_key" : "AlzaSyAA9i0G-qIVKPHAPP5wbwbeijUej9_AQpk"
"com_facebook_device_auth_instructions" : "Gå til facebook.com/device og indtast koden, som er vist ovenfor."
"com_facebook_device_auth_instructions" : "facebook.com/deviceにアクセスして、上のコードを入力してください。"
"com_facebook_device_auth_instructions" : "facebook.com/device 'ਤੇ ਵਿਜ਼ਿਟ ਕਰੋ ਅਤੇ ਉੱਪਰ ਦਿੱਤੇ ਕੋਡ ਨੂੰ ਦਾਖ਼ਲ ਕਰੋ।"
"com_facebook_device_auth_instructions" : "facebook.com/device ஐப் பார்வையிட்டு, மேலே காட்டப்பட்ட குறியீட்டை உள்ளிடவும்."
"com_facebook_device_auth_instructions" : "Gå til facebook.com/device og skriv inn koden som vises over."
"com_facebook_device_auth_instructions" : "Kunjungi facebook.com/device dan masukkan kode yang ditampilkan di atas."
"com_facebook_device_auth_instructions" : "Gehe zu facebook.com/device und gib den oben angezeigten Code ein."
"com_facebook_device_auth_instructions" : "facebook.com/deviceని సందర్శించి ఎగువన చూపిన కోడ్‌ను నమోదు చేయండి."
"com_facebook_device_auth_instructions" : "Besoek facebook.com/device en voer die kode wat hierbo gewys word, in."
"com_facebook_device_auth_instructions" : "ไปที่ facebook.com/device แล้วป้อนรหัสที่ปรากฏด้านล่าง"
"com_facebook_device_auth_instructions" : "Siirry osoitteeseen facebook.com/device ja anna oheinen koodi."

"com_facebook_device_auth_instructions" : "facebook.com/device पर विज़िट करें और ऊपर दिखाया गया कोड डालें."
"com_facebook_device_auth_instructions" : "Truy cập facebook.com/device và nhập mã được hiển thị bên trên."
"com_facebook_device_auth_instructions" : "Navštívte stránku facebook.com/device a zadajte kód zobrazený vyššie."
"com_facebook_device_auth_instructions" : "Πηγαίνετε στη διεύθυνση facebook.com/device και εισαγάγετε τον παραπάνω κωδικό."
"com_facebook_device_auth_instructions" : "facebook.com/device സന്ദർശിച്ച് മുകളിൽ കാണിച്ചിരിക്കുന്ന കോഡ് നൽകുക."
"com_facebook_device_auth_instructions" : "Ga naar facebook.com/device en voer de bovenstaande code in."
"com_facebook_device_auth_instructions" : "Odwiedź stronę facebook.com/device i wprowadź powyższy kod."
"com_facebook_device_auth_instructions" : "Puntahan ang facebook.com/device at ilagay ang code na ipinapakita sa itaas."
"com_facebook_device_auth_instructions" : "facebook.com/device দেখুন এবং উপরে দেখানো কোডটিকে প্রবেশ করান।"
"com_facebook_device_auth_instructions" : "Kunjungi facebook.com/device dan masukkan kode yang ditampilkan di bawah ini."
"com_facebook_device_auth_instructions" : "facebook.com/device ಗೆ ಭೇಟಿ ನೀಡಿ ಮತ್ತು ಮೇಲೆ ತೋರಿಸಿದ ಕೋಡ್ ಅನ್ನು ನಮೂದಿಸಿ."
"com_facebook_device_auth_instructions" : "facebook.com/device에 방문하여 위 코드를 입력하세요."
"com_facebook_device_auth_instructions" : "Vizitează facebook.com/device și introdu codul de mai sus."
"com_facebook_device_auth_instructions" : "وإدخال الرمز الموضح أعلاه facebook.com/device تفضل بزيارة"
"com_facebook_device_auth_instructions" : "Consultez facebook.com/device et entrez le code affiché ci-dessus."
"com_facebook_device_auth_instructions" : "Posjetitw facebook.com/device i unesite gore prikazani kôd."
"com_facebook_device_auth_instructions" : "facebook.com/device भेट द्या आणि वरील कोड प्रविष्ट करा."
"com_facebook_device_auth_instructions" : "facebook.com/device adresine git ve yukarıda gösterilen kodu gir "

"com_facebook_device_auth_instructions" : "facebook.com/device adresine gir ve yukarıda gösterilen kodu gir."
"com_facebook_device_auth_instructions" : "Přejděte na facebook.com/device a zadejte nahoře uvedený kód."
"com_facebook_device_auth_instructions" : "Ve a facebook.com/device e ingresa el código que se muestra arriba."
"com_facebook_device_auth_instructions" : "Lawati facebook.com/device dan masukkan kod yang ditunjukkan di atas."
"com_facebook_device_auth_instructions" : "Visita facebook.com/device e inserisci il codice mostrato qui sotto."
"com_facebook_device_auth_instructions" : "Acesse facebook.com/device e insira o código mostrado acima."
"com_facebook_device_auth_instructions" : "facebook.com/devicegt ની મુલકાત લો; અને ઉપર આપેલો કોડ દાખલ કરો."
"com_facebook_device_auth_instructions" : "Keresd fel a facebook.com/device címet, és írd be a fent megjelenített kódot."
"com_facebook_device_auth_instructions" : "Откройте facebook.com/device и введите код, показанный выше."
"com_facebook_device_auth_instructions" : "Gå till facebook.com/device och skriv in koden som visas ovan."
"com_facebook_device_auth_instructions" : "ולהזין את הקוד המוצג למעלה facebook.com/devicegt יש לבקר בכתובת"
"com_facebook_device_auth_instructions" : "Accédez à facebook.com/device et entrez le code affiché ci-dessus."
"com_facebook_device_auth_instructions" : "前往facebook.com/devicegt，並輸入上方顯示的代碼。"
"com_facebook_device_auth_instructions" : "请访问facebook.com/device并输入以上验证码。"
"com_facebook_device_auth_instructions" : "Visita facebook.com/device e introduce el código que se muestra más arriba."
"com_facebook_device_auth_instructions" : "Visita facebook.com/device e insere o código apresentado abaixo."
"com_facebook_device_auth_instructions" : "前往facebook.com/devicegt，並輸入上方顯示的代碼。"

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

此APP的危险动作

向手机申请的权限	是否危险	类型	详细情况
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储
android.permission.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备

android.permission.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
android.permission.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
android.permission.ACCESS_NETWORK_STATE	正常	查看网络状态	允许应用程序查看所有网络的状态
com.android.vending.CHECK_LICENSE	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_WIFI_STATE	正常	查看Wi-Fi状态	允许应用程序查看有关 Wi-Fi 状态的信息
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.tzt_entry.MainActivity	Schemes: https://, Hosts: paykyame.wadipanda.com, Path Prefixes: /id,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.tzt_entry,