Evaluation Warning: The document was created with Spire.Doc for Python.

**Calculator（ 2.0版本）   
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。  
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | Calculator |
| 版本 | 2.0 |
| 包名 | com.tzt\_entry |
| 域名线索 | 7条 |
| URL线索 | 8条 |
| APP图标 |  |
| 分析日期 | 2025年7月17日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

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

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| 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 |

## **4. 线索情况**

### **4.1 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 |
| www.facebook.com | IP: 205.186.152.122  所属国家: United States of America  地区: Virginia  城市: Ashburn |
| pinterest.com | IP: 157.240.10.36  所属国家: United States of America  地区: California  城市: Menlo Park |
| wap.kbzpay.com | IP: 159.138.1.199  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| twitter.com | IP: 162.159.140.229  所属国家: United States of America  地区: California  城市: San Francisco |
| codepush.appcenter.ms | 没有服务器地理信息. |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://wap.kbzpay.com/apk/sdk/download/ | com/kbzbank/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 |

### **4.3 邮箱线索**

### **4.4 手机号线索**

## **5. 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: b12153828d689f731fcaf6fe7224c25db6777575c750ad337609b92457263645887964a78a207ca92943a228e05cfcc6a36457defe4a6f0f9af233741a3ee4c1 公钥算法: rsa 密钥长度: 2048 指纹: 6a5128c903e6fe13c00adcd41edf9081e47106be9acb5a0b00976cb2e016685d**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "CodePushDeploymentKey" : "3mnVB49khmH4IAwFHvgk28AeirzRbNZ6\_KbGd2" |
| "com\_facebook\_device\_auth\_instructions" : "Visit <b>facebook.com/device</b> and enter the code shown above." |
| "google\_api\_key" : "AIzaSyAA9i0G-qlVKPHAPP5wbwbeiJUej9\_AQpk" |
| "google\_crash\_reporting\_api\_key" : "AIzaSyAA9i0G-qlVKPHAPP5wbwbeiJUej9\_AQpk" |
| "com\_facebook\_device\_auth\_instructions" : "Gå til <b>facebook.com/device</b> og indtast koden, som er vist ovenfor." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b>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" : "<b>facebook.com/device</b> 'ਤੇ ਵਿਜਿਟ ਕਰੋ ਅਤੇ ਉੱਪਰ ਦਿੱਤੇ ਕੋਡ ਨੂੰ ਦਾਖ਼ਲ ਕਰੋ।" |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> ஐப் பார்வையிட்டு, மேலே காட்டப்பட்ட குறியீட்டை உள்ளிடவும்." |
| "com\_facebook\_device\_auth\_instructions" : "Gå til <b>facebook.com/device</b> og skriv inn koden som vises over." |
| "com\_facebook\_device\_auth\_instructions" : "Kunjungi <b>facebook.com/device</b> dan masukkan kode yang ditampilkan di atas." |
| "com\_facebook\_device\_auth\_instructions" : "Gehe zu <b>facebook.com/device</b> und gib den oben angezeigten Code ein." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b>ని సందర్శించి ఎగువన చూపిన కోడ్‌ను నమోదు చేయండి." |
| "com\_facebook\_device\_auth\_instructions" : "Besoek <b>facebook.com/device</b> en voer die kode wat hierbo gewys word, in." |
| "com\_facebook\_device\_auth\_instructions" : "ไปที่ <b>facebook.com/device</b> แล้วป้อนรหัสที่ปรากฏด้านล่าง" |
| "com\_facebook\_device\_auth\_instructions" : "Siirry osoitteeseen <b>facebook.com/device</b> ja anna oheinen koodi." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> पर विज़िट करें और ऊपर दिखाया गया कोड डालें." |
| "com\_facebook\_device\_auth\_instructions" : "Truy cập <b>facebook.com/device</b> và nhập mã được hiển thị bên trên." |
| "com\_facebook\_device\_auth\_instructions" : "Navštívte stránku <b>facebook.com/device</b> a zadajte kód zobrazený vyššie." |
| "com\_facebook\_device\_auth\_instructions" : "Πηγαίνετε στη διεύθυνση <b>facebook.com/device</b> και εισαγάγετε τον παραπάνω κωδικό." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> സന്ദർശിച്ച് മുകളിൽ കാണിച്ചിരിക്കുന്ന കോഡ് നൽകുക." |
| "com\_facebook\_device\_auth\_instructions" : "Ga naar <b>facebook.com/device</b> en voer de bovenstaande code in." |
| "com\_facebook\_device\_auth\_instructions" : "Odwiedź stronę <b>facebook.com/device</b> i wprowadź powyższy kod." |
| "com\_facebook\_device\_auth\_instructions" : "Puntahan ang <b>facebook.com/device</b> at ilagay ang code na ipinapakita sa itaas." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> দেখুন এবং উপরে দেখানো কোডটিকে প্রবেশ করান৷" |
| "com\_facebook\_device\_auth\_instructions" : "Kunjungi <b>facebook.com/device</b> dan masukkan kode yang ditampilkan di bawah ini." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> ಗೆ ಭೇಟಿ ನೀಡಿ ಮತ್ತು ಮೇಲೆ ತೋರಿಸಿದ ಕೋಡ್ ಅನ್ನು ನಮೂದಿಸಿ." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b>에 방문하여 위 코드를 입력하세요." |
| "com\_facebook\_device\_auth\_instructions" : "Vizitează <b>facebook.com/device</b> şi introdu codul de mai sus." |
| "com\_facebook\_device\_auth\_instructions" : "تفضل بزيارة <b>facebook.com/device</b> وإدخال الرمز الموضح أعلاه." |
| "com\_facebook\_device\_auth\_instructions" : "Consultez <b>facebook.com/device</b> et entrez le code affiché ci-dessus." |
| "com\_facebook\_device\_auth\_instructions" : "Posjetitw <b>facebook.com/device</b> i unesite gore prikazani kôd." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> भेट द्या आणि वरील कोड प्रविष्ट करा." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> adresine git ve yukarıda gösterilen kodu gir." |
| "com\_facebook\_device\_auth\_instructions" : "Přejděte na <b>facebook.com/device</b> a zadejte nahoře uvedený kód." |
| "com\_facebook\_device\_auth\_instructions" : "Ve a <b>facebook.com/device</b> e ingresa el código que se muestra arriba." |
| "com\_facebook\_device\_auth\_instructions" : "Lawati <b>facebook.com/device</b> dan masukkan kod yang ditunjukkan di atas." |
| "com\_facebook\_device\_auth\_instructions" : "Visita <b>facebook.com/device</b> e inserisci il codice mostrato qui sotto." |
| "com\_facebook\_device\_auth\_instructions" : "Acesse <b>facebook.com/device</b> e insira o código mostrado acima." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b&gt ની મુલકાત લો; અને ઉપર આપેલો કોડ દાખલ કરો." |
| "com\_facebook\_device\_auth\_instructions" : "Keresd fel a <b>facebook.com/device</b> címet, és írd be a fent megjelenített kódot." |
| "com\_facebook\_device\_auth\_instructions" : "Откройте <b>facebook.com/device</b> и введите код, показанный выше." |
| "com\_facebook\_device\_auth\_instructions" : "Gå till <b>facebook.com/device</b> och skriv in koden som visas ovan." |
| "com\_facebook\_device\_auth\_instructions" : "יש לבקר בכתובת facebook.com/device</b&gt ולהזין את הקוד המוצג למעלה" |
| "com\_facebook\_device\_auth\_instructions" : "Accédez à <b>facebook.com/device</b> et entrez le code affiché ci-dessus." |
| "com\_facebook\_device\_auth\_instructions" : "前往<b>facebook.com/device</b&gt，並輸入上方顯示的代碼。" |
| "com\_facebook\_device\_auth\_instructions" : "请访问<b>facebook.com/device</b>并输入以上验证码。" |
| "com\_facebook\_device\_auth\_instructions" : "Visita <b>facebook.com/device</b> e introduce el código que se muestra más arriba." |
| "com\_facebook\_device\_auth\_instructions" : "Visita <b>facebook.com/device</b> e insere o código apresentado abaixo." |
| "com\_facebook\_device\_auth\_instructions" : "前往<b>facebook.com/device</b&gt，並輸入上方顯示的代碼。" |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看 |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看 |  |  |

## **9. 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 |

## **10. 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, |

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**