



MoGua

自动记账 涅槃 3.0.0 beta6.APK 分析报告



APP名称:	自动记账
包名:	cn.dreamn.qianji_auto
域名线索:	48条
URL线索:	44条
邮箱线索:	1条
分析日期:	2025年7月16日
分析平台:	摸瓜APK反编译平台

📁 文件信息

文件名: 自动记账_涅槃 3.0.0 beta6.apk
文件大小: 8.96MB
MD5值: 281fc70f96084fb366666b0b3bc2f0ef
SHA1值: 48f8bd6c972766c77f9f45e43dbfc4149186ac78
SHA256值: e9ca87aa534d39bb27f8f5c249f4fa1a918ccd2d8b414de06870f0fe0997a3c7

i APP 信息

App名称: 自动记账
包名: cn.dreamn.qianji_auto
主活动Activity: cn.dreamn.qianji_auto.ui.activity.MainActivity
安卓版本名称: 涅槃 3.0.0 beta6
安卓版本: 145

🔍 域名线索

域名	服务器信息
docs.qianjiapp.com	IP: 114.55.166.105 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
seto.teracloud.jp	IP: 103.139.238.155 所属国家: Japan 地区: Shizuoka 城市: Shizuoka 纬度: 34.983002 经度: 138.382996
apache.org	IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

schemas.android.com	没有服务器地理信息.
underscorejs.org	IP: 172.67.134.18 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
www.ankio.net	IP: 149.104.27.145 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
zenorocha.github.io	IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
mdn.alipay.com	IP: 116.142.235.232 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
ghproxy.com	IP: 144.24.81.189 所属国家: Korea (Republic of) 地区: Gangwon-do 城市: Chuncheon 纬度: 37.874722 经度: 127.734169
java.sun.com	IP: 104.126.37.152 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main 纬度: 50.110882 经度: 8.681996
pay.weixin.qq.com	IP: 220.194.111.104 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
doc.ankio.net	IP: 149.104.27.145 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
player.bilibili.com	IP: 60.213.135.86 所属国家: China 地区: Shandong 城市: Tai'an 纬度: 36.185280 经度: 117.120003

xml.apache.org	IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
tutorialzine.com	IP: 104.21.16.1 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
mmbiz.qqpic.cn	IP: 221.204.15.91 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
res.qianjiapp.com	IP: 222.134.1.29 所属国家: China 地区: Shandong 城市: Binzhou 纬度: 37.366619 经度: 118.015182
bugs.chromium.org	IP: 142.250.73.83 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
www.opensource.org	IP: 172.67.26.198 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
raw.fastgit.org	没有服务器地理信息.
www.coolapk.com	IP: 60.28.220.193 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
jqueryui.com	IP: 104.18.228.34 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
famspam.com	IP: 165.160.15.20 所属国家: United States of America 地区: Delaware 城市: Wilmington

	纬度: 39.735779 经度: -75.665703
xml.org	IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest 纬度: 29.499678 经度: -98.399246
www.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
unicode.org	IP: 64.182.27.164 所属国家: United States of America 地区: Texas 城市: Dallas 纬度: 32.814899 经度: -96.879204
cdn.jsdelivr.net	IP: 104.16.174.226 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
codemirror.net	IP: 149.210.142.219 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.378502 经度: 4.899980
wx.tenpay.com	IP: 220.196.148.65 所属国家: China 地区: Jiangsu 城市: Yancheng 纬度: 33.385559 经度: 120.125282
render.alipay.com	IP: 124.165.219.237 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
pubdav.ctfile.com	IP: 124.160.151.82 所属国家: China 地区: Zhejiang 城市: Jiaxing 纬度: 30.752199 经度: 120.750000
127.0.0.1	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000

	经度: 0.000000
marijnhaberbeke.nl	IP: 149.210.142.219 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.378502 经度: 4.899980
webdav.ctfile.com	IP: 124.160.151.82 所属国家: China 地区: Zhejiang 城市: Jiaxing 纬度: 30.752199 经度: 120.750000
raw.githubusercontent.com	IP: 185.199.109.133 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
pic.dreamn.cn	IP: 222.134.1.28 所属国家: China 地区: Shandong 城市: Binzhou 纬度: 37.366619 经度: 118.015182
snsauth.ccb.com	IP: 111.205.126.90 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
github.com	IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
qr.alipay.com	IP: 203.209.245.120 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
xmipull.org	IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
javax.xml.xmlconstants	没有服务器地理信息.
payapp.weixin.qq.com	IP: 220.194.111.104 所属国家: China 地区: Tianjin 城市: Tianjin

	纬度: 39.142181 经度: 117.176102
jshint.com	IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
open.weixin.qq.com	IP: 116.128.171.214 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
material.io	IP: 216.239.32.21 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
swiperjs.com	IP: 104.21.29.86 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
support.weixin.qq.com	IP: 182.50.12.232 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
dav.jianguoyun.com	IP: 103.52.173.35 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

 URL线索

URL信息
https://pic.dreamn.cn/uPic/2021032310470716164676271616467627123WiARFwd8b1f5bdd0fca9378a915d8531cb740b.png
https://pic.dreamn.cn/uPic/2021032310470716164676271616467627123WiARFwd8b1f5bdd0fca9378a915d8531cb740b.png
https://pic.dreamn.cn/uPic/2021032314475916164820791616482079785ssWEen
https://pic.dreamn.cn/uPic/2021032022075916162492791616249279427UY2ok6
http://res.qianjiapp.com/headerimages2/maarten-van-den-heuvel-7Ryfx2BHoXU-unsplash.jpg!headerimages2

https://qr.alipay.com/fkx18202qn4k2xono9fjk2f
https://seto.teracloud.jp/dav/
https://pubdav.ctfile.com/
https://webdav.ctfile.com/
https://dav.jianguoyun.com/dav/
https://cdn.jsdelivr.net/gh/dreamncn/AutoResource@master
https://ghproxy.com/https://raw.githubusercontent.com/dreamncn/AutoResource/master
https://raw.githubusercontent.com/dreamncn/AutoResource/master
https://raw.fastgit.org/dreamncn/AutoResource/master
https://pic.dreamn.cn/uPic/2021032310470716164676271616467627123WiARFwd8b1f5bdd0fca9378a915d8531cb740b.png
https://pic.dreamn.cn/uPic/2021032022075916162492791616249279427UY2ok6
https://www.ankio.net
https://doc.ankio.net/doc/%E8%87%AA%E5%8A%A8%E8%AE%B0%E8%B4%A6%E4%BD%BF%E7%94%A8%E6%96%87%E6%A1%A3/
https://www.coolapk.com/apk/cn.dreamn.qianji_auto
http://docs.qianjiapp.com/plugin/auto_tasker.html
https://material.io/design/components/dialogs.html
http://java.sun.com/xml/stream/properties/report-cdata-event
http://c
http://d
http://e
http://f
http://xmlpull.org/v1/doc/features.html
http://java.sun.com/xml/stream/properties/report-cdata-event
http://schemas.android.com/apk/res/android
http://schemas.android.com/android/skin
http://xml.apache.org/xslt
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Plugins

https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Error-Handling
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0
http://127.0.0.1
http://javax.xml.XMLConstants/feature/secure-processing
http://apache.org/xml/features/disallow-doctype-decl
http://apache.org/xml/features/nonvalidating/load-external-dtd
http://javax.xml.XMLConstants/property/accessExternalDTD
http://javax.xml.XMLConstants/property/accessExternalStylesheet
http://xmlpull.org/v1/doc/features.html
http://xmlpull.org/v1/doc/properties.html
http://xmlpull.org/v1/doc/features.html
http://xmlpull.org/v1/doc/features.html
http://xmlpull.org/v1/doc/properties.html
http://xmlpull.org/v1/doc/features.html
http://apache.org/xml/features/validation/dynamic
http://apache.org/xml/features/validation/schema
http://xml.org/sax/properties/declaration-handler
http://xml.org/sax/properties/lexical-handler
http://xml.org/sax/features/namespaces
http://xml.org/sax/features/namespace-prefixes
http://xml.org/sax/features/validation
http://xmlpull.org/v1/doc/features.html
http://xmlpull.org/v1/doc/features.html
http://xmlpull.org/v1/doc/properties.html
http://xmlpull.org/v1/doc/features.html

http://xmlpull.org/v1/doc/features.html
https://player.bilibili.com/player.html?aid=289448844&bvid=BV1Hf4y147Yi&cid=303785417&page=1
https://github.com/dreamncn/Qianji_auto
https://github.com/dreamncn/Qianji_auto/issues
https://doc.ankio.net/doc/%E8%87%AA%E5%8A%A8%E8%AE%B0%E8%B4%A6%E4%BD%BF%E7%94%A8%E6%96%87%E6%A1%A3/
https://codemirror.net/LICENSE
https://codemirror.net),
http://marijnhaverbeke.nl/blog/
http://unicode.org/reports/tr9/tr9-13.html
https://github.com/codemirror/CodeMirror/pull/5673
https://bugs.chromium.org/p/chromium/issues/detail?id=489206
http://marijnhaverbeke.nl/blog/codemirror-line-tree.html
https://codemirror.net/LICENSE
http://jshint.com/docs/options/
https://github.com/highlightjs/highlight.js/issues/2277
https://github.com/highlightjs/highlight.js/issues/2534
https://github.com/highlightjs/highlight.js/issues/2559
https://github.com/highlightjs/highlight.js/pull/2844
http://jqueryui.com
http://underscorejs.org
http://famspam.com/facebook/
http://www.opensource.org/licenses/mit-license.php
https://zenorocha.github.io/clipboard.js
http://tutorialzine.com/2012/02/enhance-your-website-fullscreen-api/
http://swiperjs.com
https://render.alipay.com/p/ff-fd-jblxfp45/pages/home/index.html ,topSubContent:
https://mdn.alipay.com/wsdk/img?fileId=A*ebkWSJ9yja0AAAAAAAAAAAAAfYuAQ&bz=life_app&zoom=2048w_80q_1l,link:alipays://platformapi/startapp?appId=20000032&isOpenedFund=true&tagid=YEB_INTEREST_INCOME_NOTIFY,assistName1:
https://mdn.alipay.com/wsdk/img?fileId=A*ebkWSJ9yja0AAAAAAAAAAAAAfYuAQ&bz=life_app&zoom=2048w_80q_1l,sceneExtInfo:,sceneTitle:

https://mdn.alipay.com/wsdk/img?fileid=A*K_cbS69OOIMAAAAAAAAAABkAfYuAQ&bz=life_app&zoom=2048w_80q_1l,sceneExtInfo:vipMsgNoteType:number,isProhibited:false,vip:1,sceneTitle:
https://wx.tenpay.com/cgi-bin/mmpayweb-bin/jumpuserroll?trans_id=4200001204202110013525414437&accid=085e9858ea81e8ed9d0361ea0,soundtype:0,mmreader:template_detail:template_show_type:1,text_content:cover:,color:,text:,new_tmpl_type:0,line_content:topline:value:co
https://wx.tenpay.com/cgi-bin/mmpayweb-bin/jumpuserroll?trans_id=4200001204202110013525414437&accid=085e9858ea81e8ed9d0361ea0,weapp_version:0,ext_id:,is_show_red_dot:0,hint_word:,weapp_username:,op_type:0,is_rich_text:0,word:
https://wx.tenpay.com/cgi-bin/mmpayweb-bin/jumpuserroll?trans_id=4200001204202110013525414437&accid=085e9858ea81e8ed9d0361ea0,icon_url:http://mmbiz.qpic.cn/mmbiz_png/8SAQkPMWYIB1uPsVlhric5TuWs4EPoHEjbadav39lc45Oc4IbRKulyOWuYvnicsx25ITnF37cmuULHzlcwx_fmt=png&wxfrom=200,transaction_id:4200001204202110013525414437,first_color:,title_color:,pay_style:1,finder_user_name:,pub_time:1633095300,header_jump_type:0,show_right_icon_and_desc_name:0,display_name:
https://wx.tenpay.com/cgi-bin/mmpayweb-bin/jumpuserroll?trans_id=4200001204202110013525414437&accid=085e9858ea81e8ed9d0361ea0,tweetid:,play_length:0,comment_topic_id:0,music_source:0,longurl:,styles:topColor:,style:[color:
https://wx.tenpay.com/cgi-bin/mmpayweb-bin/jumpuserroll?trans_id=100010710121100600060321701373525743&accid=085e9858ebb18158374fa8bef,soundtype:0,mmreader:template_detail:template_show_type:1,text_content:cover:,color:,text:,new_tmpl_type:0,line_content:topline
https://wx.tenpay.com/cgi-bin/mmpayweb-bin/jumpuserroll?trans_id=100010710121100600060321701373525743&accid=085e9858ebb18158374fa8bef,weapp_version:0,ext_id:,is_show_red_dot:0,hint_word:,weapp_username:,op_type:0,is_rich_text:0,word:
https://wx.tenpay.com/cgi-bin/mmpayweb-bin/jumpuserroll?trans_id=100010710121100600060321701373525743&accid=085e9858ebb18158374fa8bef,tweetid:,play_length:0,comment_topic_id:0,music_source:0,longurl:,styles:topColor:,style:[color:
https://wx.tenpay.com/userroll/readtemplate?t=userroll/index_tmpl&type=userrolldetail&trans_id=4200001200202109299385358329&create_time=1632885054,soundtype:0,mmreader:template_detail:template_show_type:1,text_content:cover:,color:,text:,new_tmpl_type:0,line_conten
https://open.weixin.qq.com/connect/oauth2/authorize?appid=wx57849631bb367f52&response_type=code&scope=snsapi_base&state=1&redirect_uri=https%3A%2F%2Fpay.weixin.qq.com%2Faction%2Findex.php%2Fmmpayentrustweb%2Fentrustweb%2Fmanager_contract%3Ftarget_page%3Ddetail%26contract_no%3D2021022457424572
https://pay.weixin.qq.com/mmpaykf/faqmanage?ver=v1&trans_id=4200001200202109299385358329&create_time=1632885054&wx_header=0&scene_code=payproof_cell,weapp_version:0,ext_id:,is_show_red_dot:0,hint_word:,weapp_username:,op_type:0,is_rich_text:0,word:
https://wx.tenpay.com/userroll/readtemplate?t=userroll/index_tmpl&type=userrolldetail&trans_id=4200001200202109299385358329&create_time=1632885054,tweetid:,play_length:0,comment_topic_id:0,music_source:0,longurl:,styles:topColor:,style:[color:
https://wx.tenpay.com/cgi-bin/mmpayweb-bin/jumpuserroll?trans_id=100004990121092900060321905318676247&accid=085e9858e772ddcd0f08c3dd6,soundtype:0,mmreader:template_detail:template_show_type:1,text_content:cover:,color:,text:,new_tmpl_type:0,line_content:topline
https://wx.tenpay.com/cgi-bin/mmpayweb-bin/jumpuserroll?trans_id=100004990121092900060321905318676247&accid=085e9858e772ddcd0f08c3dd6,weapp_version:0,ext_id:,is_show_red_dot:0,hint_word:,weapp_username:,op_type:0,is_rich_text:0,word:
https://payapp.weixin.qq.com/qrpay/qraph5/merchant/info?outtradeno=10000499012021092901324243191507,weapp_version:0,ext_id:,is_show_red_dot:0,hint_word:
https://wx.tenpay.com/cgi-bin/mmpayweb-bin/jumpuserroll?trans_id=100004990121092900060321905318676247&accid=085e9858e772ddcd0f08c3dd6,icon_url:https://wx.gtimg.com/resource/feuploader/202104/2083e7a5d5b76933c4f32dee47b88571_128x128.jpg,transaction_id:10000499012021092901324243191507,first_color:,title_color:,pa
https://wx.tenpay.com/cgi-bin/mmpayweb-bin/jumpuserroll?trans_id=100004990121092900060321905318676247&accid=085e9858e772ddcd0f08c3dd6,tweetid:,play_length:0,comment_topic_id:0,music_source:0,longurl:,styles:topColor:,style:[color:
https://support.weixin.qq.com/cgi-bin/mmsupport-bin/readtemplate?t=page/common_page__upgrade&text=text001&btn_text=btn_text_0,status:2,cache_money:
https://support.weixin.qq.com/cgi-bin/mmsupport-bin/readtemplate?t=page/common_page__upgrade&text=text001&btn_text=btn_text_0,content:,url:https://support.weixin.qq.com/cgi-bin/mmsupport-bin/readtemplate?t=page/common_page__upgrade&text=text001&btn_text=btn_t
https://snsauth.ccb.com/msg_adapter/stat_click?openid=o8QqFjIn3ubk63rhXDS4dxub43Aw&actId=SSZ32020210915183558849&tailld=TAIL_000000174320&msgType=3&headers=ygn73wgUxk%2BeeuYpySmd80e6uu50jvgFjySwSN3%2FywVaRPfWE9ombRHZrLbt08b1WBXY2FEf%2B3id2

✉ 邮箱线索

邮箱地址	所在文件
chris@ozmm.org jason@onehackoranother.com	摸瓜V2引擎

☎ 手机线索

🌟 签名证书

APK已签名
v1 签名: False
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=99, ST=dreamn, L=dreamn, O=dreamn, OU=dreamn, CN=dreamn
签名算法: rsassa_pkcs1v15
有效期自: 2020-03-26 14:42:51+00:00
有效期至: 2045-03-20 14:42:51+00:00
发行人: C=99, ST=dreamn, L=dreamn, O=dreamn, OU=dreamn, CN=dreamn
序列号: 0x756e4126
哈希算法: sha256
md5值: b0c9c2225d55202b606f2b145f4465bd
sha1值: 18c8228dcfe096491a15980b479bb89217505704
sha256值: 95dff92073e5241ce0f90a0c34e244287779a4ea3b0b02ec0c5911a031e235bf
sha512值: 8694424433349394304e9cbf2ea929175739f160853c8c85974c266cd4eb88362d45bc531770a956a301b08d1a2517b65eb05d11dc967b4bfbf3494b1fa681aa
公钥算法: rsa
密钥长度: 2048
指纹: be00fe64ab7097fcd43656d8996ba87313ed48079eb34376ff2a761996c2c8e3

🔑 硬编码敏感信息

可能的敏感信息
"dev_user" : "开发人员"
"webdav_user" : "WebDav用户名"

🔑 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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。

android.permission.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
android.permission.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
android.permission.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字

应用内通信