



MoGua

百度贴吧 12.9.3.0.APK 分析报告



APP名称:

百度贴吧

包名:	com.baidu.tieba
域名线索:	23条
URL线索:	7条
邮箱线索:	5条
分析日期:	2025年8月13日
分析平台:	摸瓜APK反编译平台

文件名: 110_95c48bc5bdae393ea3c97e74913c65df.apk
文件大小: 79.6MB
MD5值: c1b5cfbfa3026528f52e02bef16b37fb
SHA1值: 17660795b1621e1ef3b4020ffbe9df2cea4a7c10
SHA256值: 12195a8a1d3abccd6ba2815c0ba5a4c092f76f9b66ff79e5335123faefd302b2

i APP 信息

App名称: 百度贴吧
包名: com.baidu.tieba
主活动Activity: com.baidu.tieba.LogoActivity
安卓版本名称: 12.9.3.0
安卓版本: 201917184

🔍 域名线索

域名	服务器信息
ct.googleapis.com	IP: 172.217.163.42 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
query.dcdn.baidu.com	IP: 111.206.208.181 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
www.w3.org	IP: 104.18.23.19 所属国家: United States of America 地区: California

	城市: San Francisco 纬度: 37.775700 经度: -122.395203
180.76.76.112	IP: 180.76.76.112 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
vega.ws.symantec.com	没有服务器地理信息.
bdconf-turbonet.baidu.com	没有服务器地理信息.
ct.izenpe.com	IP: 194.30.98.138 所属国家: Spain 地区: Pais Vasco 城市: Derio 纬度: 43.305439 经度: -2.881160
purl.org	IP: 207.241.239.242 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.781734 经度: -122.459435
log.certly.io	没有服务器地理信息.
bdbus-turbonet.baidu.com	IP: 110.242.70.144 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
	IP: 142.251.43.14

www.webrtc.org	所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
ct.ws.symantec.com	没有服务器地理信息.
schemas.xmlsoap.org	IP: 13.107.213.74 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903
ctlog.api.venafi.com	没有服务器地理信息.
ctserver.cnnic.cn	IP: 218.241.105.21 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
crashpad.chromium.org	IP: 142.251.42.243 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
www.ietf.org	IP: 104.16.45.99 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

bdlog-turbonet.baidu.com	没有服务器地理信息.
tools.ietf.org	IP: 104.16.45.99 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
bdns.baidu.com	IP: 110.242.69.63 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
ct1.digicert-ct.com	没有服务器地理信息.
www.baidu.com	IP: 110.242.68.3 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
netlog.baidu.com	IP: 182.61.200.35 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	Url所在文件
-------	---------

<html	Mogua Engine V1
<body>	Mogua Engine V1
https://crashpad.chromium.org/bug/new	lib/armeabi/libcrashpad_handler.so
https://crashpad.chromium.org/	lib/armeabi/libcrashpad_handler.so
http://www.baidu.com	lib/armeabi/libcyber-pcdn.so
http://query.dcdn.baidu.com	lib/armeabi/libcyber-pcdn.so
http://schemas.xmlsoap.org/soap/envelope/	lib/armeabi/libcyber-pcdn.so
http://schemas.xmlsoap.org/soap/encoding/	lib/armeabi/libcyber-pcdn.so
http://purl.org/dc/elements/1.1/	lib/armeabi/libcyber-player.so
http://www.w3.org/XML/1998/namespace	lib/armeabi/libcyber-player.so
http://schemas.xmlsoap.org/soap/envelope/	lib/armeabi/libcyber-player.so
http://schemas.xmlsoap.org/soap/encoding/	lib/armeabi/libcyber-player.so
http://www.w3.org/XML/1998/namespace	lib/armeabi/libflutter.so
http://www.w3.org/2000/xmlns/	lib/armeabi/libflutter.so
https://www.w3.org/Style/CSS/Test/Fonts/Ahem/).	lib/armeabi/libflutter.so
http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor-00	lib/armeabi/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time	lib/armeabi/libjingle_peerconnection_so.so

http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01	lib/armeabi/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrext/playout-delay	lib/armeabi/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrext/video-content-type	lib/armeabi/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrext/video-timing	lib/armeabi/libjingle_peerconnection_so.so
http://tools.ietf.org/html/draft-ietf-avtext-framemarking-07	lib/armeabi/libjingle_peerconnection_so.so
http://bdlog-turbonet.baidu.com/native-log	lib/armeabi/libturbonet.so
https://ct.googleapis.com/pilot/	lib/armeabi/libturbonet.so
https://ct.googleapis.com/aviator/	lib/armeabi/libturbonet.so
https://ct1.digicert-ct.com/log/	lib/armeabi/libturbonet.so
https://ct.googleapis.com/rocketeer/	lib/armeabi/libturbonet.so
https://ct.ws.symantec.com/	lib/armeabi/libturbonet.so
https://ctlog.api.venafi.com/	lib/armeabi/libturbonet.so
https://vega.ws.symantec.com/	lib/armeabi/libturbonet.so
https://ctserver.cnnic.cn/	lib/armeabi/libturbonet.so
https://ct.izenpe.com/	lib/armeabi/libturbonet.so
https://log.certly.io/	lib/armeabi/libturbonet.so
http://netlog.baidu.com/upload.php?cuid=%s	lib/armeabi/libturbonet.so

http://bdlog-turbonet.baidu.com/log	lib/armeabi/libturbonet.so
https://bdns.baidu.com/v2/group_resolve	lib/armeabi/libturbonet.so
https://180.76.76.112/v5/0010	lib/armeabi/libturbonet.so
https://180.76.76.112/v2/0010	lib/armeabi/libturbonet.so
http://wpad/wpad.dat	lib/armeabi/libturbonet.so
http://sQUIC	lib/armeabi/libturbonet.so
https://bdbus-turbonet.baidu.com/bdbus/request	lib/armeabi/libturbonet.so
https://bdconf-turbonet.baidu.com/conf/get	lib/armeabi/libturbonet.so

 邮箱线索

邮箱地址	所在文件
wallet-kefu@baidu.com	Mogua Engine V1
4@2x.png mvp牌子@2x.png 右翅膀@2x.png	Mogua Engine V2
icon_item_toplist_16@2.6x icon_item_toplist_16@2x.webp icon_item_toplist_16@3x.webp icon_mask_post_god28@3x.webp _profile_baijiahao16@3x.webp mask_profile_bazhu16@3x.webp ask_profile_dashen16@3x.webp icon_mask_shop16@3x.webp	

deo_administration28@2x.webp
deo_administration28@3x.webp
on_mask_video_data28@2x.webp
on_mask_video_data28@3x.webp
on_mask_video_home28@2x.webp
on_mask_video_home28@3x.webp
icon_pb_right_n@2.6x
icon_pb_right_n@2x.webp
icon_pb_right_n@3x.webp
on_profile_imprint16@3x.webp
icon_profile_bluev16@3x.webp
rofile_moreimprint18@3x.webp
20slide_more24@3x.webp
n_pure_arrow12_right@3x.webp
_pure_balance_data12@2x.webp
_pure_balance_data12@3x.webp
e_barrules_careful12@3x.webp
ard_administration24@3x.webp
on_pure_card_close12@3x.webp
_pure_card_comment22@3x.webp
con_pure_card_more14@3x.webp
con_pure_card_more22@3x.webp
con_pure_card_play14@3x.webp
_pure_card_refresh16@3x.webp
on_pure_card_share22@3x.webp
_creation_question16@2.6x
_creation_question16@2x.webp
_creation_question16@3x.webp
pure_data_question16@3x.webp
icon_pure_decline12@2x.webp
icon_pure_decline12@3x.webp
ation_star_collect12@3x.webp
e_list_arrow16_right@3x.webp
e_list_arrow18_right@2x.webp
mine_shopingwindow20@3x.webp
re_personalba_lock16@3x.webp
on_pure_post_goods12@3x.webp
rofile_arrow16_right@3x.webp

re_profile_comment14@3x.webp
_pure_profile_copy14@2x.webp
_pure_profile_lock16@3x.webp
n_pure_profile_man14@2x.webp

Mogua Engine V2

pure_profile_woman14@2x.webp icon_pure_rise12@2x.webp icon_pure_rise12@3x.webp icon_pure_star_20@2.6x icon_pure_star_20@2x.webp icon_pure_star_20@3x.webp topbar_information40@3x.webp n_pure_topbar_more40@3x.webp pure_topbar_return40@3x.webp on_pure_video_data22@3x.webp _pure_video_delete22@3x.webp on_pure_video_more16@3x.webp n_pure_video_pause44@3x.webp on_pure_video_play44@3x.webp n_pure_video_share22@3x.webp _wo_recommend_copy16@2.6x con_pure_wo_yujin_20@3x.webp icon_use_item_n@3x.webp nI_digital_recommend@3x.webp k_channl_digitallist@3x.webp mask_channl_gamelist@3x.webp pic_mine_like_tost@2x.png oice_pause_filled_16@3x.webp voice_play_filled_16@2x.webp voice_play_filled_16@3x.webp	
ffmpeg-devel@ffmpeg.org	lib/armeabi/libcyber-player.so
ffmpeg-devel@ffmpeg.org	lib/armeabi/libtranscoder.so

手机线索

手机号	所在文件
19213104248	Mogua Engine V2

13680267334	Mogua Engine V2
14026093483	Mogua Engine V2

❁ 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=10000, ST=中华人民共和国, L=北京, O=百度, OU=百度贴吧
签名算法: rsassa_pkcs1v15
有效期自: 2011-10-24 10:54:28+00:00
有效期至: 3011-02-24 10:54:28+00:00
发行人: C=10000, ST=中华人民共和国, L=北京, O=百度, OU=百度贴吧
序列号: 0x4ea543e4
哈希算法: sha1
md5值: 673004cf2f6efdec2385c8116c1e8c14
sha1值: 4d482a419ea0d47af9fb6a3221525900bc77b3b2
sha256值: 81e69ceb1b2566d435ecd5173b9ad0370c8e7b01760ac5c7e6b559266a221193
sha512值: 980b656ce83cec98e1ed22941b22a343028f89bba9a1e76bc4d77b83d01ff50a33086441d19757ae67f19a35b0c0fa0e3412e466ac2798b59a5df6e46a2d2ddb
公钥算法: rsa
密钥长度: 1024
指纹: 11dcc3d55636cf4faa38c7329e4768b95b8da18b1ed403eccf59eeca318d5ab3

🔑 硬编码敏感信息

可能的敏感信息
"aiapp_menu_authority_management" : "权限管理"
"aiapp_menu_global_private" : "全部私信"

"aiapps_anti_addiction_dialog_auth" : "去认证"
"aiapps_authenticate_fail" : "当前账号无操作权限"
"aiapps_http_authentication_login" : "登录"
"aiapps_http_authentication_password" : "密码"
"aiapps_http_authentication_username" : "姓名"
"aiapps_open_histroy_private_mode" : "搜索历史"
"aiapps_setting_scope_auth_failed" : "授权请求失败"
"aiapps_ssl_certificate" : "安全证书"
"aiapps_view_certificate" : "查看证书"
"ala_person_live_real_authen" : "实名认证"
"ala_person_live_real_authen_authenticated" : "已认证"
"ala_person_live_real_authen_denied" : "已拒绝"
"ala_person_live_real_authen_in_review" : "审核中"
"ala_person_live_real_authen_unauthorized" : "未认证"
"anti_account_modifypwd_tip" : "您的账号存在安全风险，请及时修改密码"
"at_username" : "@%1\$s: "
"bd_wallet_auth_cancel_auth" : "确认"
"hd_wallet_auth_card_need_detail" : "卡信息需补全"

bd_wallet_auth_card_need_detail : "卡信息需补全"
"bd_wallet_auth_check_xieyi" : "请先勾选度小满一键支付协议"
"bd_wallet_auth_primary_pay_method" : "优先支付方式"
"bd_wallet_auth_sel_bank_card_tip" : "请选择优先扣费银行卡"
"bd_wallet_auth_submit_sign" : "确认开通"
"bd_wallet_balance_pwd_setting_tip2" : "为了你的账户安全，请设置手机支付密码"
"bd_wallet_base_to_input_pay_pwd" : "请输入手机支付密码"
"bd_wallet_fingerprint_auth_failed" : "指纹验证失败"
"bd_wallet_fingerprint_no_pwd_tips" : "你尚未设置手机支付密码，不能开启指纹支付功能！ "
"bd_wallet_fingerprint_set_pwd" : "设置支付密码"
"bd_wallet_fingerprint_use_pwd" : "请使用密码继续支付"
"bd_wallet_passfree_no_pwd_tips" : "你尚未设置手机支付密码，不能开启小额免密功能！ "
"bd_wallet_pay_pwd_free_pp" : "小额免密支付"
"bd_wallet_pay_security_auth" : "实名认证"
"block_user" : "拉黑"
"common_menu_authority_management" : "权限管理"
"default_user_name" : "贴吧会员"
"dxm_wallet_auth_card_need_detail" : "卡信息需补全"

"dxm_wallet_auth_check_xieyi": "请先勾选度小满一键支付协议"
"dxm_wallet_auth_sel_bank_card_tip": "请选择优先扣费银行卡"
"dxm_wallet_base_set_pwd_click": "点我开启"
"dxm_wallet_base_set_pwd_tips": "你还没有设置六位支付密码，暂不能使用余额进行支付"
"dxm_wallet_base_to_input_pay_pwd": "请输入手机支付密码"
"dxm_wallet_do_auth": "去实名"
"dxm_wallet_pay_pwd_free_pp": "小额免密支付"
"ebpay_auth_payresult_pay_success": "开通并支付成功"
"ebpay_auth_payresult_sign_success": "开通成功"
"ebpay_certificate": "身份证"
"ebpay_check_pwd": "安全验证"
"ebpay_check_pwd_close_hce": "安全确认"
"ebpay_check_pwd_close_showcode": "安全确认"
"ebpay_check_pwd_modify_pwd": "修改支付密码"
"ebpay_check_pwd_save": "保存设置"
"ebpay_find_password": "找回密码"
"ebpay_find_pwd_get_cardlist_failed": "获取卡列表失败，请重试"
"ebpay_intermediarypay_pwdcheck": "支付密码"

"ebpay_intermediarypay_pwdcheck_tip": "请输入支付密码"
"ebpay_please_input_pwd1": "输入密码完成支付"
"ebpay_please_input_pwd2": "输入密码以添加银行卡"
"ebpay_pwd_changed": "密码不一致，请重新输入"
"ebpay_pwd_check_sub_tip_for_bind_or_complete_card": "请输入支付密码，以添加银行卡"
"ebpay_pwd_check_sub_tip_for_close_hce": "请输入支付密码，以暂停云闪付"
"ebpay_pwd_check_sub_tip_for_close_showcode": "请输入支付密码，以暂停付款码服务"
"ebpay_pwd_check_sub_tip_for_complete_pay": "请输入支付密码，以完善信息"
"ebpay_pwd_check_sub_tip_for_open_hce": "请输入支付密码，以开通云闪付"
"ebpay_pwd_check_sub_tip_for_save": "请输入支付密码，以保存设置"
"ebpay_pwd_check_sub_tip_for_unbind_card": "请输入支付密码，以解绑银行卡"
"ebpay_pwd_check_sub_tip_for_verify": "请输入支付密码，以验证身份"
"ebpay_pwd_check_tip": "请输入支付密码，以验证身份"
"ebpay_pwd_check_tip_close_showcode": "输入密码暂停付款码服务"
"ebpay_pwd_check_tip_modify_pwd": "请输入旧密码"
"ebpay_pwd_check_tip_save": "请输入支付密码，以保存设置"
"ebpay_pwd_check_tip_unbind_card": "请输入支付密码，以解绑银行卡"

"ebpay_pwd_check_title": "验证支付密码"
"ebpay_pwd_close_promotion_dialog": "我知道了"
"ebpay_pwd_confim_tip_pay": "请设置支付密码并支付"
"ebpay_pwd_done": "完成"
"ebpay_pwd_explain": "支付密码说明"
"ebpay_pwd_forget": "忘记密码"
"ebpay_pwd_set_tip": "请设置6位支付密码"
"ebpay_pwd_to_pay": "密码支付"
"ebpay_pwd_use_explain": "什么是支付密码"
"ebpay_pwdpay_balance_tips": "本单可用 %1\$s元"
"ebpay_pwdpay_balance_txt": "余额 %1\$s元"
"ebpay_pwdpay_credit_tips": "可用额度 %1\$s元"
"ebpay_pwdpay_payment_select": "选择支付方式"
"ebpay_set_pwd_success": "新密码设置成功"
"fans_default_name_god_user": "粉丝: %1\$s"
"forum_detail_private_apply_failed": "吧务申请失败"
"forum_detail_private_apply_left_num_tip": "吧务剩余%1\$s个名额未申请"
"forum_detail_private_applying": "吧务申请中"

"frs_private_add_manager" : "添加吧务"
"frs_private_apply_rule" : "吧规申请"
"frs_private_fail_button" : "重新创建"
"frs_private_manager_approval" : "吧务审批"
"frs_private_success_title" : "恭喜您"
"fun_ad_item_authority" : "权限"
"god_authentication" : "大神认证"
"group_info_author" : "群主"
"host_not_authority" : "当前域名下，无权限调用该端能力"
"image_water_show_user_name" : "显示用户名"
"input_tdou_password" : "请输入T豆支付密码"
"item_download_authority" : "权限"
"ksad_ad_default_author" : "@可爱的广告君创造的原声"
"ksad_ad_default_username" : "@可爱的广告君"
"modify_pwd" : "修改密码"
"more_info_username" : "Ta的用户名"%1\$s""
"pb_history_default_user_name" : "主播"

"pb_history_user_name" : "%s的直播间"
"pb_private" : "评论权限"
"pb_private_block_title" : "1作者设置了评论权限，仅展示作者自己的评论"
"person_auth_perfix" : "认证： %s"
"person_center_auth_desc" : "百度认证： "
"private_bar_complaint" : "吧投诉"
"private_desc" : "仅自己可见"
"private_secret" : "私密"
"sailor_ssl_certificate" : "安全证书"
"sailor_view_certificate" : "查看证书"
"secret_full_browse_mode_tips" : "我们非常重视您的个人信息保护。关于个人信息收集和使用的详细信息，在使用百度贴吧前，请您认真查阅《隐私政策》和《用户协议》，您同意并接受全部条款后再使用我们的服务。 "
"setup_password" : "设置支付密码"
"star_cover_pic_author" : "头图 / @%1\$s"
"star_cover_post_author" : "头条 / @%1\$s"
"swan_bookshelf_authorize_fail" : "授权失败"
"swanapp_auth_and_login" : "授权登录"
"swanapp_auth_dialog_phone_explain" : "绑定的手机号码"

"swanapp_auth_dialog_userinfo_explain" : "用户公开信息"
"swanapp_auth_switch_tip" : "授权【%s】获取手机号"
"swanapp_hover_dialog_auth" : "前往开启"
"swanapp_hover_dialog_not_auth" : "暂不开启"
"swanapp_multi_auth_agreement_desc" : "已阅读并同意以下协议"
"swanapp_multi_auth_default_name_end" : " 获取以下信息为您服务"
"swanapp_multi_auth_default_name_head" : "授权 "
"swanapp_multi_auth_guest_login_name_head" : "登录并授权 "
"swanapp_multi_auth_un_realname_name_head" : "实名认证并授权 "
"swanapp_unchecked_auth_tip" : "授权登录需要使用您的手机号"
"tansmit_bjh_author_name" : "@%1\$s:"
"tb_err_token_expired" : "令牌过期，请稍后再试"
"tb_token" : "贴口令"
"tdou_password" : "T豆支付密码"
"tip_init_user_name" : "Hi，补充用户名后才能继续操作哦~"
"tip_private_assist_apply" : "吧务申请"
"topic_pk_user" : "%1\$s +1"
"user" : "用户名"

"wallet_base_set_pwd_click" : "点我开启"
"wallet_base_set_pwd_tips" : "你还没有设置六位支付密码，暂不能使用余额进行支付"
"wallet_cashdesk_pwd_pay" : "密码支付"
"wallet_do_auth" : "去实名"
"wallet_fp_changed_usepwd" : "您手机录入的指纹发生变化，为了保障您的支付安全，本次请您使用密码支付"
"wallet_hce_do_auth" : "去实名"
"wrong_password" : "输入的密码有误"
"youngster_settings_input_password" : "请输入密码"
"youngster_settings_set_password" : "设置密码"
"youngster_settings_verify_password" : "确认密码"

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

🗨 应用内通信

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