



山东理工大学 SDLG_3.2.0.APK 分析报告



APP名称:

山东理工大学

包名: `com.lysoft.android.lyyd.report.mobile.sdlg`

域名线索: 25条

URL线索: 7条

邮箱线索: 0条

分析日期: 2025年6月17日

分析平台: [摸瓜APK反编译平台](#)

文件名: 山东理工大学 SDLG_3.2.0 com.lysoft.android.lyyd.report..apk
文件大小: 50.17MB
MD5值: 88c255b42380b1759f77388e87443ef7
SHA1值: 314aadf20a4f4d28754f1f1344ee18230ba07345
SHA256值: 931be80ad5da5019e29bd2a263771f2ee740cbdfbcbf16eae65fc47c70357867

i APP 信息

App名称: 山东理工大学
包名: com.lysoft.android.lyyd.report.mobile.sdlg
主活动Activity: com.lysoft.android.lyyd.report.config.dispatch.DispatchActivity
安卓版本名称: SDLG_3.2.0
安卓版本: 64

🔍 域名线索

域名	服务器信息
data-dre.push.dbankcloud.com	IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel 纬度: 54.321358 经度: 10.134532
metrics1.data.hicloud.com	IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
grs.dbankcloud.com	IP: 60.28.200.159 所属国家: China 地区: Tianjin

	城市: Tianjin 纬度: 39.142181 经度: 117.176102
store-dra.hispace.dbankcloud.com	IP: 222.73.142.47 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
www.yibaogao.com	IP: 119.91.66.47 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
grs.dbankcloud.asia	IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
data-drru.push.dbankcloud.com	IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
grs.dbankcloud.eu	没有服务器地理信息.
data-dra.push.dbankcloud.com	IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987

	经度: 103.850281
ydxyllysky.com	IP: 119.91.66.47 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
mcp.sdut.edu.cn	IP: 211.64.23.131 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
appgallery.cloud.huawei.com	IP: 121.36.118.136 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
www.mob.com	IP: 180.188.26.28 所属国家: China 地区: Zhejiang 城市: Taizhou 纬度: 28.666668 经度: 121.349998
metrics5.data.hicloud.com	IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
store-at-dre.hispace.dbankcloud.com	没有服务器地理信息.

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
store-drru.hispace.dbankcloud.com	IP: 159.138.201.153 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
store-drcn.hispace.dbankcloud.cn	IP: 111.202.17.15 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
play.google.com	IP: 59.24.3.174 所属国家: Korea (Republic of) 地区: Gyeonggi-do 城市: Seongnam 纬度: 37.420624 经度: 127.126717
data-drcn.push.dbankcloud.com	IP: 121.36.117.8 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
metrics-dra.dt.hicloud.com	IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987

	经度: 103.850281
grs.dbankcloud.cn	IP: 124.70.116.153 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
store-dre.hispace.dbankcloud.com	IP: 222.73.142.45 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
yibaogao.com	IP: 119.91.66.47 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
metrics2.data.hicloud.com	IP: 80.158.2.190 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel 纬度: 54.321358 经度: 10.134532

 URL线索

URL信息	Url所在文件
https://yibaogao.com/ybg_share_icon.png	摸瓜V1引擎

https://www.yibaogao.com	摸瓜V1引擎
http://mcp.sdut.edu.cn:8080	摸瓜V1引擎
https://play.google.com/store/apps/details?id=	摸瓜V1引擎
https://appgallery.cloud.huawei.com	摸瓜V1引擎
https://github.com/vinc3m1	摸瓜V1引擎
https://github.com/vinc3m1/RoundedImageView	摸瓜V1引擎
https://github.com/vinc3m1/RoundedImageView.git	摸瓜V1引擎
http://www.mob.com/policy/en>http://www.mob.com/policy/en.	摸瓜V1引擎
http://www.mob.com/about/policy>http://www.mob.com/about/policy	摸瓜V1引擎
http://www.mob.com	摸瓜V1引擎
https://ydx.y-sky.com:8098	摸瓜V1引擎
https://www.yibaogao.com/yibaogao_ui/help.html	摸瓜V1引擎
http://www.yibaogao.com/	摸瓜V1引擎
http://www.mob.com/policy/zh>http://www.mob.com/policy/zh	摸瓜V1引擎
http://www.mob.com/about/policy/en>http://www.mob.com/about/policy/en.If	摸瓜V1引擎
https://store-at-dre.hispace.dbankcloud.com/hwmarket/api/	摸瓜V2引擎
https://metrics1.data.hicloud.com:6447	摸瓜V2引擎
https://metrics-dra dt hicloud.com:6447	摸瓜V2引擎

https://metrics-dra.dt.hicloud.com:6447/	摸瓜V2引擎
https://metrics2.data.hicloud.com:6447	摸瓜V2引擎
https://metrics5.data.hicloud.com:6447	摸瓜V2引擎
https://data-drcn.push.dbankcloud.com	摸瓜V2引擎
https://data-dra.push.dbankcloud.com	摸瓜V2引擎
https://data-dre.push.dbankcloud.com	摸瓜V2引擎
https://data-drru.push.dbankcloud.com	摸瓜V2引擎
https://metrics1.data.hicloud.com:6447	摸瓜V2引擎
https://metrics-dra.dt.hicloud.com:6447	摸瓜V2引擎
https://metrics2.data.hicloud.com:6447	摸瓜V2引擎
https://metrics5.data.hicloud.com:6447	摸瓜V2引擎
https://store-drcn.hispace.dbankcloud.cn/hwmarket/api/	摸瓜V2引擎
https://store-dra.hispace.dbankcloud.com/hwmarket/api/	摸瓜V2引擎
https://store-dre.hispace.dbankcloud.com/hwmarket/api/	摸瓜V2引擎
https://store-drru.hispace.dbankcloud.com/hwmarket/api/	摸瓜V2引擎
https://grs.dbankcloud.com	摸瓜V2引擎
https://grs.dbankcloud.cn	摸瓜V2引擎
https://grs.dbankcloud.eu	摸瓜V2引擎

 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=CN, ST=广东省, L=广州市, O=数字化校园事业部, OU=广州联奕信息科技有限公司, CN=www.ly-sky.com
签名算法: rsassa_pkcs1v15
有效期自: 2013-08-15 14:50:25+00:00
有效期至: 2040-12-31 14:50:25+00:00
发行人: C=CN, ST=广东省, L=广州市, O=数字化校园事业部, OU=广州联奕信息科技有限公司, CN=www.ly-sky.com
序列号: 0x60600a76
哈希算法: sha256
md5值: 82aa029d74a1b89b369bde5e3c6faabf
sha1值: 7e18c73078f82ddde20bb228d4aef74f17c9a950
sha256值: 8d177ebe46415c4084866024d680e2c68eba03ddd38429db1c7cd4ebb118d6bb
sha512值: 805f9500df5a4e1e34d917ed506f336ff107bfa8360b46c0da0fa9cddef6d90894971c9dc4e6cd7e4812fe4a3c99b9c55616bf18132f91e15cd5722cb9407ccb
公钥算法: rsa
密钥长度: 2048
指纹: 0269723bee67760e04da50791087417a0df696dddc7f825fc08688d7f77ea6bb

 硬编码敏感信息

可能的敏感信息

"forgetpassword" : "OPz,忘记密码了吗"
"library_roundedimageview_author" : "Vince Mi"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"mobcommon_authorize_dialog_accept" : "Accept"
"mobcommon_authorize_dialog_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click http://www.mob.com/policy/en. If you agree with our service policy, please click accept, if you do not agree with our service policy, please click reject"
"mobcommon_authorize_dialog_reject" : "Reject"
"mobcommon_authorize_dialog_title" : "Terms of Use"
"mobdemo_authorize_dialog_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见http://www.mob.com/about/policy。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"
"mobdemo_authorize_dialog_title" : "服务授权"
"mobile_api" : "mobileapi_ydxy"
"mobile_campus_private_chat_list" : "私聊列表"
"mobile_campus_private_group_list" : "群列表"
"mobile_campus_route_personal_modifyPwd" : "/personal/modifyPwd"
"mobile_campus_router_my_gesture_pwd_setting" : "/my/GesturePwdSettingActivity"
"mobile_campus_router_my_gesture_pwd_verify" : "/my/GesturePwdVerifyActivity"
"modifypassword" : "修改密码"
"my_password" : "修改密码"

"my_private" : "隐私管理"
"no_user" : "该用户未登录过，暂时无法联系"
"password" : "请输入您的密码"
"please_input_password" : "请输入密码"
"private_chat" : "私信"
"ssdk_cmcc_auth" : "手机认证服务由中国移动提供"
"ssdk_cmcc_login_one_key" : "本机号码一键登录"
"ssdk_instapaper_pwd" : "密码"
"ssdk_weibo_oauth_regiseter" : "应用授权"
"mobcommon_authorize_dialog_accept" : "同意"
"mobcommon_authorize_dialog_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见 http://www.mob.com/policy/zh。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"</td'>
"mobcommon_authorize_dialog_reject" : "拒绝"
"mobcommon_authorize_dialog_title" : "服务授权"
"mobcommon_authorize_dialog_accept" : "Accept"
"mobcommon_authorize_dialog_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click <a accept,="" agree="" click="" do="" href="http://www.mob.com/policy/en>http://www.mob.com/policy/en." if="" not="" our="" please="" policy,="" reject"<="" service="" td="" with="" you="">
"mobcommon_authorize_dialog_reject" : "Reject"

"mobcommon_authorize_dialog_title" : "Terms of Use"
"mobdemo_authorize_dialog_content" : "In order to provide you with Mobservice related products and services, please check our privacy policy in detail, see detailshttp://www.mob.com/about/policy/en.If you agree with our privacy policy, please click accept. If you disagree with our privacy policy, please click reject."
"mobdemo_authorize_dialog_title" : "service authority"
"ssdk_cmcc_auth" : "Provided by China Mobile"
"ssdk_cmcc_login_one_key" : "PhoneNum Login"
"ssdk_instapaper_pwd" : "Password"
"ssdk_weibo_oauth_regiseter" : "Authorization"

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.USE_FINGERPRINT	正常	allow use of指纹	该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE_BIOMETRIC
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
android.permission.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
android.permission.WRITE_CONTACTS	危险	写入联系人数据	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据
android.permission.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
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.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_CALENDAR	危险	读取日历事件	允许应用程序读取您手机上存储的所有日历事件。恶意应用程序可以借此将您的日历事件发送给其他人
android.permission.WRITE_CALENDAR	危险	添加或修改日历事件并向客人发	允许应用程序添加或更改日历上的事件,这可能会向客人发送电子邮件。恶意应用程序可以使用它来删除或修改您的日历活动或

		送电子邮件	向客人发送电子邮件
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.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.ACCESS_FINE_LOCATION	危险	精细定位 (GPS)	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置(如果可用)。恶意应用程序可以使用它来确定您的大致位置
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
android.permission.BROADCAST_PACKAGE_ADDED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_CHANGED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_INSTALL	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_REPLACED	未知	Unknown permission	Unknown permission from android reference
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
android.permission.CHANGE_NETWORK_STATE	正	更改网络连接	允许应用程序更改网络连接状态。

	常		
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
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
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
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.READ_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等
android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
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.CAMERA	危险	拍照和录像	允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像
android.permission.WAKE_LOCK	正	防止手机睡眠	允许应用程序防止手机进入睡眠状态

	常		
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.WRITE_MEDIA_STORAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_AUDIO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。
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
	正		

android.permission.RESTART_PACKAGES	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.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
com.sec.android.provider.badge.permission.READ	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.UPDATE_SHORTCUT	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.anddoes.launcher.permission.UPDATE_COUNT	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或徽章
com.majeur.launcher.permission.UPDATE_BADGE	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或标记为固体。
com.huawei.android.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章
com.huawei.android.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章
android.permission.READ_APP_BADGE	正	显示应用程序通	允许应用程序显示应用程序图标徽章

	常	知	
com.oppo.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
me.everything.badger.permission.BADGE_COUNT_READ	未知	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	未知	Unknown permission	Unknown permission from android reference
com.lysoft.android.lyyd.report.mobile.sdlg.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
com.lysoft.android.lyyd.report.mobile.sdlg.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	Unknown permission	Unknown permission from android reference
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

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.lysoft.android.report.mobile_campus.module.launch.view.MobileCampusSSOActivity	Schemes: sdlg://,

	Hosts: mobile.campus.sso,
com.lysoft.android.lyyd.report.baselibrary.framework.sdk.umeng.MipushTestActivity	Schemes: agoo://, Hosts: com.lysoft.android.lyyd.report.mobile.sdlg, Paths: /thirdpush,
cn.sharesdk.tencent.qq.ReceiveActivity	Schemes: tencent://,
cn.sharesdk.loopshare.LoopShareActivity	Schemes: ssdk://, Hosts: cn.sharesdk.loop,

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。