MoGua

安全教育平台 1.8.7.APK 分析报告

APP名称:	安全教育平台

包名:	com.jzzs.ParentsHelper
域名线索:	7条
URL线索:	5条
邮箱线索:	0条
分析日期:	2024年4月26日
分析平台:	摸瓜反编译平台

文件信息

文件名: com.jzzs.ParentsHelper_v1.8.7_2265.com.apk
文件大小: 18.75MB
MD5值: e08a1baeadc07a07e9c9f59dd9717c83
SHA1值: 8712495250354218d4d862b7d6cde06d0f80ef25
SHA256值: 883b2923f07ca02aa36d5920266849900e3e7b3ebbc6bb9e90a1d56989673a22

APP 信息

App名称: 安全教育平台
包名: com.jzzs.ParentsHelper
主活动Activity: com.jzzs.ParentsHelper.WelcomeActivity
安卓版本名称: 1.8.7
安卓版本: 1006026

域名线索

域名	服务器信息
github.com	**IP**: 20.205.243.166 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
store.hispace.hicloud.com	**IP**: 49.4.32.127 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
appgallery.cloud.huawei.com	**IP**: 117.78.15.51 **所属国家**: China **地区**: Guangdong

	城市: Guangzhou **纬度**: 23.116671 **经度**: 113.250000
errlogos.umeng.com	**IP**: 47.246.110.96 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
lame.sf.net	**IP**: 204.68.111.100 **所属国家**: United States of America **地区**: California **城市**: San Diego **纬度**: 32.799797 **经度**: -117.137047
errlog.umeng.com	**IP**: 223.109.148.142 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
play.google.com	**IP**: 172.217.163.46 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514

URL线索

URL**信息**	Url**所在文件**

https://play.google.com/store/apps/details?id=	Android String Resource
https://appgallery.cloud.huawei.com	Android String Resource
https://github.com/vinc3m1	Android String Resource
https://github.com/vinc3m1/RoundedImageView	Android String Resource
https://github.com/vinc3m1/RoundedImageView.git	Android String Resource
https://store.hispace.hicloud.com/hwmarket/api/	Android String Resource
https://errlog.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi-v7a/libcrashsdk.so
https://errlogos.umeng.com	lib/armeabi-v7a/libcrashsdk.so
http://lame.sf.net	lib/arm64-v8a/liblame.so
https://errlog.umeng.com/api/crashsdk/logcollect	lib/arm64-v8a/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/arm64-v8a/libcrashsdk.so
https://errlog.umeng.com	lib/arm64-v8a/libcrashsdk.so
https://errlogos.umeng.com	lib/arm64-v8a/libcrashsdk.so
https://errlog.umeng.com/api/crashsdk/logcollect	lib/armeabi/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/armeabi/libcrashsdk.so

https://errlog.umeng.com	lib/armeabi/libcrashsdk.so
https://errlogos.umeng.com	lib/armeabi/libcrashsdk.so

邮箱线索

手机线索

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=CN, ST=浙江, L=杭州, O=杭州安康应急教育有限公司, CN=谭迎虎
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-03-07 10:27:48+00:00
Valid To: 2116-02-12 10:27:48+00:00
Issuer: C=CN, ST=浙江, L=杭州, O=杭州安康应急教育有限公司, CN=谭迎虎
Serial Number: 0xc2174ec
Hash Algorithm: sha256
md5: bd84c74da0006b0b6282ba9fdf612710
sha1: 21e96aa73dabdb93c2c74cb42a710c9fdb154c3d
sha256: c9233d94b0a3833ffa6923b16fb8bca46bd38d19ff3604b9eb4e66e89d53ebbf
sha512: 3daa6fa07cdbf19cd1e7877caf4f1311429a01491ab2c353c9602f0823c08aa0d33cd0ebe1caf76ca21dceb7c059dbf96c23457a8e6ea4365e9a51427d58af46
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: ee4ebc318b2336936897abbe64530b87f2406405c449e5703822ae59d6e3c5c3

硬编码敏感信息

可能的敏感信息
"library_roundedimageview_author" : "Vince Mi"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"login_please_input_pwd" : "请输入您的密码"

加壳分析

加壳类型	所属文件
360	libjiagu.so

第三方SDK

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.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
	正	发送粘性广	允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导

android.permission.BROADCAST_STICKY	常	播	致手机使用过多内存,从而使手机运行缓慢或不稳定
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.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.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.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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.SCHEDULE_EXACT_ALARM	正常		允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作
getui.permission.GetuiService.com.jzzs.ParentsHelper	未知	Unknown permission	Unknown permission from android reference
com.jzzs.ParentsHelper.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
com.jzzs.ParentsHelper.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference
com.jzzs.ParentsHelper.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.push.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference

com.meizu.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.jzzs.ParentsHelper.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.jzzs.ParentsHelper.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.permission.PUSH	未知	Unknown permission	Unknown permission from android reference
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.jzzs.ParentsHelper.MainActivity	Schemes: xueanquanpublish://, Hosts: route.xueanquan.com,
com.tencent.tauth.AuthActivity	Schemes: tencent1106099616://,