MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

单位换算宝 Failed.APK

APP名称:	单位换算宝
包名:	Failed
域名线索:	10条
URL线索:	21条
邮箱线索:	0条
分析日期:	2022年2月2日 19:44

文件信息

文件名: dwhsb538535.apk
文件大小: 6.2MB
MD5值: ac6c682c97601d2d687c258fda27c86d
SHA1值: 2b13b1bdc37b1abb19a81684d129c41473a9c20c
SHA256值: e7b59d6a3ce43d8258251ad33635b8df672158e461c74d91165a90f5ad794af0

APP 信息

App名称: 单位换算宝
包名: Failed
主活动Activity:
安卓版本名称: Failed
安卓版本: Failed

域名线索

域名	是否危险域名	服务器信息
user-gold-cdn.xitu.io	good	没有服务器地理信息.
www.xnln.net	good	**IP:** 67.225.218.6 **所属国家:** United States of America **地区:** Michigan **城市:** Lansing **纬度:** 42.733280 **经度:** -84.637764 **查看地图:** Google Map
photocdn.sohu.com	good	**IP:** 182.40.19.215 **所属国家:** China **地区:** Shandong **城市:** Qingdao **纬度:** 36.098610 **经度:** 120.371941 **查看地图:** Google Map

域名	是否危险域名	服务器信息
p6-juejin.byteimg.com	good	**IP:** 42.202.162.113 **所属国家:** China **地区:** Liaoning **城市:** Dandong **纬度:** 40.129169 **经度:** 124.394722 **查看地图:** Google Map
gitee.com	good	**IP:** 212.64.62.183 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看地图:** Google Map
juejin.im	good	**IP:** 103.136.220.204 **所属国家:** Singapore **地区:** Singapore **城市:** Singapore **纬度:** 1.289670 **经度:** 103.850067 **查看地图:** Google Map
gl-apk.oss-cn-qingdao.aliyuncs.com	good	**IP:** 47.104.37.163 **所属国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423 **查看地图:** Google Map

域名	是否危险域名	服务器信息
mp.weixin.qq.com	good	**IP:** 175.24.209.30 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看地图:** Google Map
github.com	good	**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 **查看地图:** Google Map
schemas.android.com	good	没有服务器地理信息.

URL线索

URL信息	Url所在文件
http://photocdn.sohu.com/tvmobilemvms/20150907/144160323071011277.jpg	com/lida/danweihuansuan/utils/DemoDataProvider.java
http://photocdn.sohu.com/tvmobilemvms/20150907/144158380433341332.jpg	com/lida/danweihuansuan/utils/DemoDataProvider.java
http://photocdn.sohu.com/tvmobilemvms/20150907/144160286644953923.jpg	com/lida/danweihuansuan/utils/DemoDataProvider.java
http://photocdn.sohu.com/tvmobilemvms/20150902/144115156939164801.jpg	com/lida/danweihuansuan/utils/DemoDataProvider.java
http://photocdn.sohu.com/tvmobilemvms/20150907/144159406950245847.jpg	com/lida/danweihuansuan/utils/DemoDataProvider.java

URL信息	Url所在文件
http://mp.weixin.qq.com/mp/homepage?__biz=Mzg2NjA3NDIyMA==&hid=5&sn=bdee5aafe9cc2e0a618d055117c84139&scene=18#wechat_redirect	com/lida/danweihuansuan/utils/DemoDataProvider.java
https://p6-juejin.byteimg.com/tos-cn-i-k3u1fbpfcp/463930705a844f638433d1b26273a7cf~tplv-k3u1fbpfcp-watermark.image	com/lida/danweihuansuan/utils/DemoDataProvider.java
https://juejin.im/post/5c3ed1dae51d4543805ea48d	com/lida/danweihuansuan/utils/DemoDataProvider.java
https://user-gold-cdn.xitu.io/2019/1/16/1685563ae5456408?imageView2/0/w/1280/h/960/format/webp/ignore-error/1	com/lida/danweihuansuan/utils/DemoDataProvider.java
https://juejin.im/post/5b480b79e51d45190905ef44	com/lida/danweihuansuan/utils/DemoDataProvider.java
https://user-gold-cdn.xitu.io/2018/7/13/16492d9b7877dc21?imageView2/0/w/1280/h/960/format/webp/ignore-error/1	com/lida/danweihuansuan/utils/DemoDataProvider.java
https://juejin.im/post/5b6b9b49e51d4576b828978d	com/lida/danweihuansuan/utils/DemoDataProvider.java
https://user-gold-cdn.xitu.io/2018/8/9/1651c568a7e30e02?imageView2/0/w/1280/h/960/format/webp/ignore-error/1	com/lida/danweihuansuan/utils/DemoDataProvider.java
https://juejin.im/post/5c6fc0cdf265da2dda694f05	com/lida/danweihuansuan/utils/DemoDataProvider.java
https://user-gold-cdn.xitu.io/2019/2/22/16914891cd8a950a?imageView2/0/w/1280/h/960/format/webp/ignore-error/1	com/lida/danweihuansuan/utils/DemoDataProvider.java
https://gitee.com/	com/lida/danweihuansuan/utils/sdkinit/XBasicLibInit.java
https://github.com/xuexiangjys	com/lida/danweihuansuan/core/webview/AgentWebFragment.java
https://github.com/xuexiangjys	com/lida/danweihuansuan/core/webview/XPageWebViewFragment.java
http://www.xnln.net/app/addCommentXui.php	com/lida/danweihuansuan/fragment/other/YjfkFragment.java

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	com/xuexiang/xui/widget/banner/widget/banner/base/BaseBanner.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Observable.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0#error-handling	io/reactivex/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
http://gl-apk.oss-cn-qingdao.aliyuncs.com/html/yhxy/yhxy_danweihuansuanbao.html	Android String Resource
http://gl-apk.oss-cn-qingdao.aliyuncs.com/html/yszc/yszc_danweihuansuanbao.html	Android String Resource

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=US, O=Android, CN=Android Debug
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-03-14 07:18:29+00:00
Valid To: 2042-03-07 07:18:29+00:00
Issuer: C=US, O=Android, CN=Android Debug
Serial Number: 0x4f604645
Hash Algorithm: sha1

md5: b721f8716643ed250c7da015e6140b80
sha1: 1baa659d9ed232924a2344b5de9b9bed58b49dd5
sha256: c2e2fb02e362aa8cc9255df9a8aef770f43a48d7d0b84a6b3d27c1ed6e56c7d9
sha512: 3d2e5b29d0d0f3e591cd108b37cc247d52fa20a724d3d303fe2b7f3cb7e2972ee017ac580d4328d7648ecc13dd6e310d815b1ffa19eca556610ce1ec6eb222c4

硬编码敏感信息

可能的敏感信息
"about_item_author_github" : "联系作者"
"lab_forget_password" : "忘记密码?"
"lab_login_by_password" : "密码登录"
"regex_password" : "^(?:(?=.*[a-zA-Z])(?=.*[0-9])).{8,18}$"

加壳分析

文件列表	分析结果
classes.dex	壳列表 / 详细情况 反虚拟机: Build.FINGERPRINT check Build.MANUFACTURER check Build.BOARD check 反调试: Debug.isDebuggerConnected() check 编译器: r8

文件列表	分析结果
classes2.dex	壳列表 | 详细情况 编译器 | r8 without marker (suspicious)
