MoGua

Health Code Demo 1.5.3.APK 分析报告



APP名称: Health Code Demo

包名:	org.pix.healthcode
域名线索:	2条
URL线索:	3条
邮箱线索:	0条
分析日期:	2024年3月28日
分析平台:	摸瓜反编译平台

文件信息

文件名: HealthCode.apk

文件大小: 0.31MB
MD5值: 00d44ead94d095dfd985399d62a20191
SHA1值: 0b640b1e397082b760b77b9e71f12dfa38a1c67c
SHA256值: 5fb599b8f8309cd8c963432f977375c90e6e3d6a2561f78795fe44aa6cbb73d0

APP 信息

App名称: Health Code Demo
包名: org.pix.healthcode
主活动Activity: org.pix.healthcode.MainActivity
安卓版本名称: 1.5.3
安卓版本: 1019

域名线索

域名	服务器信息
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
morrowind.github.io	**IP**: 185.199.110.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065632 **经度**: -79.891708

URL线索

URL信息	Url所在文件
https://play.google.com/store/apps/	org/pix/healthcode/WebViewActivity.java
https://morrowind.github.io/privacypolicy/health-code-demo.html	org/pix/healthcode/MainActivity.java
https://play.google.com/store/apps/details?id=org.pix.healthcode	Mogua Engine V1

邮箱线索

手机线索

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=CN, ST=ZJ, L=HZ, O=LXG, OU=DEV, CN=Morrowind.Xie
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2000-01-01 08:15:18+00:00
Valid To: 2099-12-31 08:15:18+00:00
Issuer: C=CN, ST=ZJ, L=HZ, O=LXG, OU=DEV, CN=Morrowind.Xie
Serial Number: 0x5948b83c
Hash Algorithm: sha256
md5: a783074b4f2bc21d220449e3f5273dc2
sha1: 7c6561d8c4785aa1a527d9e7fdfa25c5f1ea6667
sha256: cd4da30f24f33cac24e0b58fc6f4ad87793e48ce0c43244870f9509ebf0aa33a
sha512: 4755610c8229ac8ce8747acc3485c55335ee7d5f186fc5be8a1a56a5efec2e45829d244005355211d3a7d408d935b2174579ff403bf262b558b0a4a5753c857e

硬编码敏感信息

可能的敏感信息
"key_info" : "Personal Info"
"key_location" : "Location Info"
"key_other" : "Other Info"
"menu_author" : "Author"
"menu_edit_user" : "Edit Person %1$d Info"
"user_name" : "Full name"
"key_info" : "个人资料"
"key_location" : "位置信息"
"key_other" : "其它设置"
"menu_author" : "开发者"
"menu_edit_user" : "编辑申领人%1$d信息"
"user_name" : "姓名"

加壳分析

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.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

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。