MoGua

测试DEMO MINI 1.0.APK 分析报告

APP名称:	测试DEMO MINI

包名:	com.unionpay.plugin.demo.mini
域名线索:	16条
URL线索:	2条
邮箱线索:	0条
分析日期:	2025年6月8日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: UPVerifyDemoMini.apk
文件大小: 0.4MB
MD5值: 5385458584fdb44629ff0092124b2535
SHA1值: 3414b3e71f3832acaf0ea4e843ad5f53fde349d9
SHA256值: a4932fcff9d9d54bbe347439b347fa53eb0c625b23e2bc524d9c5bcda3fff2c8

APP 信息

App名称: 测试DEMO MINI
包名: com.unionpay.plugin.demo.mini
主活动Activity: com.unionpay.plugin.demo.MainActivity
安卓版本名称: 1.0
安卓版本: 1

域名线索

域名	服务器信息
appcashier.test.95516.com	**IP**: 111.161.121.254 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
172.18.64.34	**IP**: 172.18.64.34 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
	IP: 101.231.114.217 **所属国家**: China **地区**: Shanghai

101.231.114.217	**城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
appcashier.test.cup.com.cn	**IP**: 123.125.46.38 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
202.101.25.178	**IP**: 202.101.25.178 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
appcashier256.csstest.cup.com.cn	没有服务器地理信息.
172.21.135.13	**IP**: 172.21.135.13 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
101.231.114.216	**IP**: 101.231.114.216 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
172.17.236.157	**IP**: 172.17.236.157 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000

	经度: 0.000000
acpstatic.95516.com	**IP**: 123.126.74.16 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
101.231.204.84	**IP**: 101.231.204.84 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
appcashier256.csstest.unionpay.com	**IP**: 101.231.114.194 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
172.20.51.34	**IP**: 172.20.51.34 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
172.17.236.159	**IP**: 172.17.236.159 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
	IP: 60.9.3.148 **所属国家**: China

acpstatic.cup.com.cn	**地区**: Hebei **城市**: Hengshui **纬度**: 37.732220 **经度**: 115.701157
172.21.131.12	**IP**: 172.21.131.12 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000

URL线索

URL信息	Url所在文件
http://172.20.51.34:8087	com/unionpay/configs/Configs.java
http://172.20.51.34:8087/sim/app.jsp?user=admin	com/unionpay/configs/Configs.java
http://172.18.64.34:10305/sim/app.jsp?user=admin	com/unionpay/configs/Configs.java
http://172.17.236.157:8087/sim/app.jsp?user=admin	com/unionpay/configs/Configs.java
http://172.21.131.12:10305/sim/app.jsp?user=admin	com/unionpay/configs/Configs.java
http://172.21.135.13:10000/para/getRedis	com/unionpay/configs/Configs.java
http://101.231.114.216:1725/sim/app.jsp?user=admin	com/unionpay/configs/Configs.java
http://101.231.114.217:8080/sim/app.jsp?user=admin	com/unionpay/configs/Configs.java
http://172.17.236.159:8087/sim/gettnb?t=1	com/unionpay/configs/Configs.java

http://172.17.236.159:8087/sim/gettnb?t=6y	com/unionpay/configs/Configs.java
http://172.17.236.159:8087/sim/gettnb?t=6z	com/unionpay/configs/Configs.java
http://101.231.204.84:8091/sim/getacptn	com/unionpay/configs/Configs.java
http://202.101.25.178:8080/sim/gettn	com/unionpay/configs/Configs.java
https://appcashier.test.95516.com/gateway/mobile/json	lib/armeabi/libentryexpro.so
https://appcashier256.csstest.unionpay.com/gateway/mobile/json	lib/armeabi/libentryexpro.so
https://appcashier.test.95516.com/app/mobile/json	lib/armeabi/libentryexpro.so
https://appcashier256.csstest.unionpay.com/app/mobile/json	lib/armeabi/libentryexpro.so
https://appcashier.test.95516.com/app/mobile/hft	lib/armeabi/libentryexpro.so
https://appcashier256.csstest.unionpay.com/app/mobile/hft	lib/armeabi/libentryexpro.so
https://appcashier.test.95516.com/app/mobile/conf	lib/armeabi/libentryexpro.so
https://appcashier256.csstest.unionpay.com/app/mobile/conf	lib/armeabi/libentryexpro.so
https://appcashier.test.cup.com.cn/app/mobile/conf	lib/armeabi/libentryexpro.so
https://appcashier256.csstest.cup.com.cn/app/mobile/conf	lib/armeabi/libentryexpro.so
https://acpstatic.95516.com/gw/app/scan/android//%s.json	lib/armeabi/libentryexpro.so
https://appcashier256.csstest.unionpay.com/gw/app/scan/android/%s.json	lib/armeabi/libentryexpro.so
https://acpstatic.cup.com.cn/gw/app/scan/android//%s.json	lib/armeabi/libentryexpro.so
https://appcashier256.csstest.cup.com.cn/gw/app/scan/android/%s.json	lib/armeabi/libentryexpro.so

https://appcashier.test.95516.com/app/mobile/callingapp	lib/armeabi/libentryexpro.so
https://appcashier256.csstest.unionpay.com/app/mobile/callingapp	lib/armeabi/libentryexpro.so
https://appcashier.test.cup.com.cn/app/mobile/callingapp	lib/armeabi/libentryexpro.so
https://appcashier256.csstest.cup.com.cn/app/mobile/callingapp	lib/armeabi/libentryexpro.so
https://acpstatic.95516.com/gw/app/cashierdesk/scan/android/%s.json	lib/armeabi/libentryexpro.so
https://appcashier256.csstest.unionpay.com/gw/app/cashierdesk/scan/android/%s.json	lib/armeabi/libentryexpro.so
https://acpstatic.cup.com.cn/gw/app/cashierdesk/scan/android/%s.json	lib/armeabi/libentryexpro.so
https://appcashier256.csstest.cup.com.cn/gw/app/cashierdesk/scan/android/%s.json	lib/armeabi/libentryexpro.so

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=200000, ST=sh, L=sh, O=up, OU=up, CN=tp
签名算法: rsassa_pkcs1v15
有效期自: 2017-08-31 07:12:38+00:00
有效期至: 2017-11-29 07:12:38+00:00
发行人: C=200000, ST=sh, L=sh, O=up, OU=up, CN=tp

序列号: 0x187217f9
哈希算法: sha256
md5值: aa31fc145b2f078883a766a61de4bd99
sha1值: 91f87ebd3f471fc60347169ec6594ffb3644fba7
sha256值: 94c56addd32144046f529a81be01137f68b92deed60574c88cb591dc18e8eaef
sha512值: ca3ef78123d1fb8173ee9d9c055facfaa014be6d7ce457915103528af4d5794ff01c24c4b2d0151bf5e5b123f4c7acec2731f8c8ab3a120ddffb1ba72717e196
公钥算法: rsa
密钥长度: 2048
指纹: a7bc5858808b95483972e5275fcfb45969c04aaba5491be4b35fcb271789997c

硬编码敏感信息

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	类型	详细情况

	危险		
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.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.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
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_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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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
org.simalliance.openmobileapi.SMARTCARD	未知	Unknown permission	Unknown permission from android reference
android.permission.NFC	正常	控制近场通信	允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信

应用内通信