



## ANDROID STATIC ANALYSIS REPORT



 WiGLE WiFi Wardriving FOSS  
(2.29)

File Name: installer173.apk

Package Name: net.wigle.wigleandroid






Scan Date: May 30, 2022, 4:27 p.m.

App Security Score: 30/100 (HIGH RISK)

Grade:



## FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
11	13	1	1	2

## FILE INFORMATION

File Name: installer173.apk

Size: 3.21MB

MD5: f17caacf39762fe6f7a3e5d5c17efb62

SHA1: b58b9adff5c9ab2c3e226bcfcdf43cae7d5e8b84

SHA256: 28ec10da3b4b3643e033ad064442f5207221ac1e3cb106b28113621d56847b5d

## APP INFORMATION

App Name: WiGLE WiFi Wardriving FOSS

Package Name: net.wigle.wigleandroid

Main Activity: net.wigle.wigleandroid.MainActivity

Target SDK: 27

Min SDK: 14

Max SDK:

Android Version Name: 2.29

Android Version Code: 229

## APP COMPONENTS

Activities: 10

Services: 1

Receivers: 4

Providers: 1

Exported Activities: **2**

Exported Services: 0

Exported Receivers: **4**

Exported Providers: 0

## CERTIFICATE INFORMATION

APK is signed

v1 signature: True

v2 signature: False

v3 signature: False

Found 1 unique certificates

Subject: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid

Signature Algorithm: rsassa\_pkcs1v15

Valid From: 2012-10-16 19:34:54+00:00

Valid To: 2040-03-03 19:34:54+00:00

Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid

Serial Number: 0x507db6de

Hash Algorithm: sha1

md5: 38cfa1cfc1eeac453cb23dc53fc7d85d

sha1: 82f4cb091bbde751f99e69ef358877d6a767b721

sha256: 699dbee594797d7efb681f625620ec1e41e41e6a57afdcd8533f8d22003529e8

sha512: a5900490f923eec41d9aab473771f6675660e302ec10addb9cfe5acf7303633bac338832dd68e6c48fde0bf4b3e0e9c288671812c6235ee4ab1b243e474629ad

TITLE	SEVERITY	DESCRIPTION
Signed Application	<a href="#">info</a>	Application is signed with a code signing certificate

TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	high	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Certificate algorithm might be vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

## ≡ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
net.wigle.wigleandroid.permission.MAPS_RECEIVE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.

## APKID ANALYSIS

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.PRODUCT check Build.BOARD check
	Compiler	r8 without marker (suspicious)

## NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

## MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Launch Mode of Activity (net.wigle.wigleandroid.MainActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
3	Activity (net.wigle.wigleandroid.ActivateActivity) is not Protected. An intent-filter exists.	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.
4	Launch Mode of Activity (net.wigle.wigleandroid.ErrorReportActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
5	Launch Mode of Activity (net.wigle.wigleandroid.SpeechActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
6	Launch Mode of Activity (net.wigle.wigleandroid.NetworkActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
7	Activity (net.wigle.wigleandroid.RegistrationActivity) is not Protected. An intent-filter exists.	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.



NO	ISSUE	SEVERITY	DESCRIPTION
8	Launch Mode of Activity (net.wigle.wigleandroid.FilterActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
9	Launch Mode of Activity (net.wigle.wigleandroid.MacFilterActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
10	Launch Mode of Activity (net.wigle.wigleandroid.MapFilterActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
11	Launch Mode of Activity (net.wigle.wigleandroid.DBResultActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
12	Broadcast Receiver (net.wigle.wigleandroid.listener.TerminationReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
13	Broadcast Receiver (net.wigle.wigleandroid.listener.UploadReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
14	Broadcast Receiver (net.wigle.wigleandroid.listener.ScanControlReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
15	Broadcast Receiver (net.wigle.wigleandroid.listener.StartWigleAtBootReciever) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.

## </> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	<a href="#">The App logs information. Sensitive information should never be logged.</a>	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	net/wigle/wigleandroid/MainActivity.java org/slf4j/helpers/Util.java net/wigle/wigleandroid/ActivateActivity.java br/com/sapereaude/maskedEditText/MaskedEditText.java net/wigle/wigleandroid/background/ObservationImporter.java org/slf4j/impl/AndroidLoggerAdapter.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	<a href="#">App can read/write to External Storage. Any App can read data written to External Storage.</a>	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	net/wigle/wigleandroid/MainActivity.java net/wigle/wigleandroid/DatabaseHelper.java net/wigle/wigleandroid/background/ObservationUploader.java net/wigle/wigleandroid/ErrorMessageReportActivity.java
3	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	net/wigle/wigleandroid/MainActivity.java
4	<a href="#">Files may contain hardcoded sensitive information like usernames, passwords, keys etc.</a>	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	net/wigle/wigleandroid/NewsFragment.java net/wigle/wigleandroid/UploadsFragment.java net/wigle/wigleandroid/RankListAdapter.java net/wigle/wigleandroid/RankStatsFragment.java net/wigle/wigleandroid/ListFragment.java net/wigle/wigleandroid/NetworkActivity.java
5	<a href="#">App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.</a>	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	net/wigle/wigleandroid/background/QueryThread.java net/wigle/wigleandroid/DatabaseHelper.java
6	<a href="#">Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.</a>	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	net/wigle/wigleandroid/RegistrationActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
----	-------	----------	-----------	-------

7	<a href="#">Remote WebView debugging is enabled.</a>	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	net/wigle/wigleandroid/RegistrationActivity.java
---	--	------	--	--

## SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
----	---------------	----	-----------------	-------	-------	---------	---------	---------------------

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/mips/libpl_droidsonroids_gif.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>Partial RELRO <a href="#">warning</a></p> <p>This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/armeabi-v7a/libpl_droidsonroids_gif.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>Full RELRO <a href="#">info</a></p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/mips64/libpl_droidsonroids_gif.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>Partial RELRO <a href="#">warning</a></p> <p>This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	lib/x86/libpl_droidsonroids_gif.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>Full RELRO <a href="#">info</a></p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	lib/arm64-v8a/libpl_droidsonroids_gif.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>Partial RELRO <a href="#">warning</a></p> <p>This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	lib/armeabi/libpl_droidsonroids_gif.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>Full RELRO <a href="#">info</a></p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	lib/x86_64/libpl_droidsonroids_gif.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>Full RELRO <a href="#">info</a></p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	<a href="#">FCS_RBG_EXT.1.1</a>	Security Functional Requirements	Random Bit Generation Services	The application use no DRBG functionality for its cryptographic operations.
2	<a href="#">FCS_STO_EXT.1.1</a>	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	<a href="#">FCS_CKM_EXT.1.1</a>	Security Functional Requirements	Cryptographic Key Generation Services	The application implement asymmetric key generation.
4	<a href="#">FDP_DEC_EXT.1.1</a>	Security Functional Requirements	Access to Platform Resources	The application has access to ['camera', 'location', 'network connectivity'].
5	<a href="#">FDP_DEC_EXT.1.2</a>	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	<a href="#">FDP_NET_EXT.1.1</a>	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	<a href="#">FDP_DAR_EXT.1.1</a>	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
8	<a href="#">FMT_MEC_EXT.1.1</a>	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	<a href="#">FTP_DIT_EXT.1.1</a>	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
10	FCS_CKM.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Asymmetric Key Generation	The application generate asymmetric cryptographic keys not in accordance with FCS_CKM.1.1(1) using key generation algorithm RSA schemes and cryptographic key sizes of 1024-bit or lower.
11	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.

## DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
maps.google.com	ok	IP: 216.58.208.110 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: <a href="#">Google Map</a>
api.wigle.net	ok	IP: 54.70.85.50 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
www.opengis.net	ok	IP: 66.244.86.70 Country: United States of America Region: Indiana City: Jasper Latitude: 38.391441 Longitude: -86.931107 View: <a href="#">Google Map</a>
wigle.net	ok	IP: 54.70.85.50 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: <a href="#">Google Map</a>
javax.xml.xmlconstants	ok	No Geolocation information available.
schemas.android.com	ok	No Geolocation information available.
www.slf4j.org	ok	IP: 83.166.144.67 Country: Switzerland Region: Geneve City: Carouge Latitude: 46.180962 Longitude: 6.139210 View: <a href="#">Google Map</a>



EMAIL	FILE
wiwiwa@wiple.net	net/wiple/wipleandroid/ErrorMessageActivity.java

## HARDCODED SECRETS

POSSIBLE SECRETS
"crypto_password" : "Password"
"crypto_password" : "パスワード"
"crypto_show_password" : "パスワードを表示します。"
"setting_show_password" : "パスワードを表示する"
"status_no_user" : "ユーザ名が設定されていません"
"auth_username" : "Benutzerautorisierung"
"crypto_password" : "Passwort"
"crypto_password" : "סיסמה"
"auth_username" : "授权用户"
"crypto_password" : "密码"
"crypto_show_password" : "显示密码。"

POSSIBLE SECRETS
"password" : "WiGLE密码"
"setting_show_password" : "显示密码"
"status_no_user" : "用户名未设置, 转到设置"
"username" : "WiGLE名"
"crypto_password" : "Salasana"
"crypto_password" : "पासवर्ड"
"crypto_password" : "Wachtwoord"
"password" : "WiGLE-wachtwoord"
"username" : "WiGLE-gebruikersnaam"
"crypto_password" : "Hasło"
"crypto_password" : "Password"
"crypto_password" : "암호"
"crypto_password" : "Passord"
"crypto_password" : "Password"
"auth_username" : "Authentication"
"crypto_password" : "Parola"



POSSIBLE SECRETS
"crypto_password" : "Heslo"
"crypto_password" : "Contraseña"
"password" : "Contraseña"
"auth_username" : "Autenticato"
"crypto_password" : "Password"
"crypto_password" : "Senha"
"crypto_password" : "Jelszó"
"crypto_password" : "Пароль"
"crypto_password" : "Lösenord"
"crypto_password" : "Wachtwurd"
"password" : "WiGLE-wachtwurd"
"username" : "WiGLE-brûkersnamme"
"crypto_password" : "密碼"
"crypto_show_password" : "顯示密碼。"
"password" : "WiGLE密碼"
"setting_show_password" : "顯示密碼"

POSSIBLE SECRETS
"status_no_user" : "用戶名不設定"
"username" : "WiGLE名"
"auth_username" : "授权用户"
"crypto_password" : "密码"
"crypto_show_password" : "显示密码。"
"password" : "WiGLE密码"
"setting_show_password" : "显示密码"
"status_no_user" : "用户名未设置，转到设置"
"username" : "WiGLE名"
"crypto_password" : "Senha"
"crypto_password" : "密碼"
"crypto_show_password" : "顯示密碼。"
"password" : "WiGLE密碼"
"setting_show_password" : "顯示密碼"
"status_no_user" : "用戶名不設定"
"username" : "WiGLE名"

---

## Report Generated by - MobSF v3.5.2 Beta

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.

© 2022 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).