APP SCORES

Security Score 32/100

Trackers Detection 0/432

FILE INFORMATION

File Name OWASP_GoatDroid-_FourGoats_Android_App.apk

Size 1.2MB

MD5 969bac4cb8392ceb79b5e60f310e480b

SHA1 414da9666c83dcbfdd984eb60ddc57dd69cb06bf

SHA256 35b126c88069521735fc65dc49b003276b3978ffeae3f901d80bb98c558c82f0

APP INFORMATION

App Name FourGoats

Package Name org.owasp.goatdroid.fourgoats

Main Activity .activities.Main

Target SDK 15 **Min SDK** 9 **Max SDK**

Android Version Name 1.0 **Android Version Code** 1

3 / 33

EXPORTED ACTIVITIES

View All

1 / 1

EXPORTED SERVICES

View All

1 / 1

EXPORTED RECEIVERS

View All

0 / 0

EXPORTED PROVIDERS

View All

SCAN OPTIONS

DECOMPILED CODE

SIGNER CERTIFICATE

```
Binary is signed
v1 signature: True
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: O=OWASP, OU=Mobile, CN=OWASP GoatDroid
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-09-23 16:28:58+00:00
Valid To: 2062-09-11 16:28:58+00:00
Issuer: O=OWASP, OU=Mobile, CN=OWASP GoatDroid
Serial Number: 0x505f38ca
Hash Algorithm: sha1
md5: 75e5cddbba1a08e474ca1835ea0b40be
sha1: 719aff5671daeb7217d18732f57dc8343da515cf
sha256: 80146542b63af23e1bb9b2024f6f5aa6a9df6578e46ee3b3faee76ca4a0cb238
sha512: 1b065a628c3db760794a2b485beb3c29168a889e7432a482f49ff6d6af228806dd7a4cdd9225cdca9e8982e054d16cda940708e84c3cadc47fe5aacccc14f4c9
Found 1 unique certificates
```

APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
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.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.	
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.	
android.permission.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.	

Showing 1 to 5 of 5 entries

Previous 1 Next

ANDROID API

Search:

API	FILES
Certificate Handling	
Dynamic Class and Dexloading	
Get Installed Applications	
Get System Service	

API	FILES
GPS Location	org/owasp/goatdroid/fourgoats/fragments/DoCheckin.java org/owasp/goatdroid/fourgoats/services/LocationService.java
HTTP Requests, Connections and Sessions	
Inter Process Communication	
Java Reflection	
Local File I/O Operations	
Send SMS	

Showing 1 to 10 of 15 entries

Previous 1 2 Next

BROWSABLE ACTIVITIES

Search:

ACTIVITY	INTENT
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

NETWORK SECURITY

Search:

NO	SCOPE	SEVERITY	DESCRIPTION
No data available in table			

Showing 0 to 0 of 0 entries

Previous Next

CERTIFICATE ANALYSIS

HIGH	WARNING	INFO
2	0	1

Search:

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.
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.

Showing 1 to 3 of 3 entries

Previous 1 Next

MANIFEST ANALYSIS

HIGH	WARNING	INFO	SUPPRESSED
5	6	0	0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable unpatched Android version 2.3-2.3.2, [minSdk=9]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.	
2	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.	
3	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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.	
4	Activity (.activities.ViewCheckin) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (15) of the app to 29 or higher to fix this issue at platform level.	
5	Activity (.activities.ViewCheckin) is not Protected. [android:exported=true]	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.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
6	Activity (.activities.ViewProfile) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (15) of the app to 29 or higher to fix this issue at platform level.	
7	Activity (.activities.ViewProfile) is not Protected. [android:exported=true]	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.	
8	Activity (.activities.SocialAPIAuthentication) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (15) of the app to 29 or higher to fix this issue at platform level.	
9	Activity (.activities.SocialAPIAuthentication) is not Protected. [android:exported=true]	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.	
10	Service (.services.LocationService) is not Protected. An intent-filter exists.	warning	A Service 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 Service is explicitly exported.	

Showing 1 to 10 of 11 entries

Previous 1 2 Next

</> CODE ANALYSIS

HIGH	WARNING	INFO	SECURE	SUPPRESSED
3	3	1	1	0

Search:

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
1	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	**CWE:** CWE-749: Exposed Dangerous Method or Function **OWASP Top 10:** M1: Improper Platform Usage **OWASP MASVS:** MSTG-PLATFORM-7		
2	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	**CWE:** CWE-295: Improper Certificate Validation **OWASP Top 10:** M3: Insecure Communication **OWASP MASVS:** MSTG-NETWORK-3	org/owasp/goatdroid/fourgoats/requestresponse/CustomSSLSocketFactory.java	
3	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	**OWASP MASVS:** MSTG-NETWORK-4	org/owasp/goatdroid/fourgoats/requestresponse/CustomSSLSocketFactory.java	
4	The App logs information. Sensitive information should never be logged.	info	**CWE:** CWE-532: Insertion of Sensitive Information into Log File **OWASP MASVS:** MSTG-STORAGE-3		
5	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.	warning	**CWE:** CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') **OWASP Top 10:** M7: Client Code Quality	org/owasp/goatdroid/fourgoats/db/CheckinDBHelper.java org/owasp/goatdroid/fourgoats/db/UserInfoDBHelper.java	

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
6	The file or SharedPreference is World Readable. Any App can read from the file	high	**CWE:** CWE-276: Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS:** MSTG-STORAGE-2	org/owasp/goatdroid/fourgoats/misc/Utils.java	
7	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	**CWE:** CWE-312: Cleartext Storage of Sensitive Information **OWASP Top 10:** M9: Reverse Engineering **OWASP MASVS:** MSTG-STORAGE-14	com/actionbarsherlock/internal/view/menu/MenuBuilder.java	
8	Debug configuration enabled. Production builds must not be debuggable.	high	**CWE:** CWE-919: Weaknesses in Mobile Applications **OWASP Top 10:** M1: Improper Platform Usage **OWASP MASVS:** MSTG-RESILIENCE-2	org/owasp/goatdroid/fourgoats/BuildConfig.java	

Showing 1 to 8 of 8 entries

Previous 1 Next

SHARED LIBRARY BINARY ANALYSIS

No Shared Objects found.

Search:

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
No data available in table									

Showing 0 to 0 of 0 entries

Previous Next

NIAP ANALYSIS v1.3

Search:

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
No data available in table				

Showing 0 to 0 of 0 entries

Previous Next

FILE ANALYSIS

Search:

NO	ISSUE	FILES
No data available in table		

Showing 0 to 0 of 0 entries

Previous Next

FIREBASE DATABASE ANALYSIS

Search:

TITLE	SEVERITY	DESCRIPTION
No data available in table		

Showing 0 to 0 of 0 entries

Previous Next

MALWARE LOOKUP

VirusTotal Report | Triage Report | MetaDefender Report | Hybrid Analysis Report

APKiD ANALYSIS

Search:

DEX	DETECTIONS
classes.dex	Search:

FINDINGS	DETAILS
Compiler	dx

Showing 1 to 1 of 1 entries

Previous 1 Next

Showing 1 to 1 of 1 entries

Previous 1 Next

BEHAVIOUR ANALYSIS

Search:

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/actionbarsherlock/widget/ActivityChooserModel.java
00091	Retrieve data from broadcast	collection	
00193	Send a SMS message	sms	org/owasp/goatdroid/fourgoats/activities/SendSMS.java org/owasp/goatdroid/fourgoats/broadcastreceivers/SendSMSNowReceiver.java org/owasp/goatdroid/fourgoats/javascriptinterfaces/SmsJSInterface.java

Showing 1 to 3 of 3 entries

Previous 1 Next

ABUSED PERMISSIONS

Top Malware Permissions	4/25	Other Common Permissions	1/44
android.permission.SEND_SMS, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.INTERNET		android.permission.CALL_PHONE	

Malware Permissions are the top permissions that are widely abused by known malware.
Other Common Permissions are permissions that are commonly abused by known malware.

SERVER LOCATIONS

DOMAIN MALWARE CHECK

URLS

EMAILS

TRACKERS

Search:

TRACKER NAME	CATEGORIES	URL
No data available in table		

Showing 0 to 0 of 0 entries

Previous Next

POSSIBLE HARDCODED SECRETS

STRINGS

From APK Resource

From Code

▶ Show all **486** strings

From Shared Objects

ACTIVITIES

▼ Showing all **33** activities

.activities.Main
.activities.Login
.activities.Register
.activities.Home
.fragments.DoCheckin

.activities.Checkins
.activities.Friends
.fragments.HistoryFragment
.activities.History
.activities.Rewards
.activities.AddVenue
.activities.ViewCheckin
.fragments.MyFriends
.fragments.SearchForFriends
.activities.ViewProfile
.fragments.PendingFriendRequests
.activities.ViewFriendRequest
.fragments.MyRewards
.fragments.AvailableRewards
.activities.Preferences
.activities.About
.activities.SendSMS
.activities.DoComment
.activities.UserHistory
.activities.DestinationInfo
.activities.AdminHome
.activities.AdminOptions
.fragments.ResetUserPasswords
.fragments.DeleteUsers
.activities.DoAdminPasswordReset
.activities.DoAdminDeleteUser
.activities.SocialAPIAuthentication
.activities.GenericWebViewActivity

SERVICES

▼ Showing all **1** services
.services.LocationService

RECEIVERS

▼ Showing all **1** receivers
.broadcastreceivers.SendSMSNowReceiver

PROVIDERS

LIBRARIES

SBOM

▼ Showing all **2** Packages
com.actionbarsherlock
org.owasp.goatdroid.fourgoats

FILES

► Show all **361** files

Version v4.4.5