

Assignment 6 – Static Analysis (Android & iOS)

1. Static Analysis of Android App

(A.) Allsafe

✓ Information

all basic info about application

The screenshot displays the Allsafe static analysis tool interface. The top navigation bar includes links for RECENT SCANS, STATIC ANALYZER, DYNAMIC ANALYZER, API, DONATE, DOCS, and ABOUT. The main content area is divided into several sections:

- APP SCORES:** Shows a security score of 49/100 and a track record of 0/432. A MobSP Scorecard is also visible.
- FILE INFORMATION:** Lists file details for 'allsafe.apk', including size (10.39MB), MD5, SHA1, and SHA256 hashes.
- APP INFORMATION:** Provides details about the app, including package name (infosecadventures.allsafe), main activity (infosecadventures.allsafe.MainActivity), target SDK (35), min SDK (23), max SDK (35), and Android version (1.5).
- EXPORTED ACTIVITIES, SERVICES, RECEIVERS, PROVIDERS:** Each section shows a count of exported items (2/4, 1/2, 2/2, and 1/4 respectively) and a 'View All' link.
- SCAN OPTIONS:** Includes buttons for Rescan, Manage Suppressions, Start Dynamic Analysis, and Scan Logs.
- DECOMPILED CODE:** Offers options to view AndroidManifest.xml, View Source, View Smali, Download Java Code, Download Smali Code, and Download APK.

✓ SIGNER CERTIFICATE

issue:- using only v1 and v2 certificate that not much secure

The screenshot shows the SIGNER CERTIFICATE section of the static analysis tool. It indicates that the binary is signed and lists the following details:

- Binary is signed
- v1 signature: True
- v2 signature: True
- v3 signature: False
- v4 signature: False
- Subject: CN=Android Debug, O=Android, C=US
- Signature Algorithm: sha256WithRSAEncryption
- Valid From: 2022-06-28 07:49:58+00:00
- Valid To: 2052-06-28 07:49:58+00:00
- Issuer: CN=Android Debug, O=Android, C=US
- Serial Number: 0x1
- Hash Algorithm: sha1
- MD5: ece2f3a0793095b0918e5c4a0d40109
- SHA1: 44a3f480ce08e5e6c7daed70948917aa1d4309f7
- SHA256: b1c87b4883a70ff61f28061df640285cbf613705a3b59670c3e942cbaadb8ae
- SHA512: 4671248e3a30527846dc24f05ed5ef0996a8f1f74723660997bfb8ed167c3343b8be3800a9b25092bf08e9437b267b7e7f376620140971fb49fb2b62b3
- Publickey Algorithm: rsa
- Bit Size: 2048
- Fingerprint: d4d90c07153a31571dc15583b541cbc51bd51e27c7b0191d7b0706a5303256d
- Found 1 unique certificates

✓ APPLICATION PERMISSIONS

issue: unwanted permission as shown in ss

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.	Show Files
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.	
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.	Show Files
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.	Show Files
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.	Show Files
android.permission.QUERY_ALL_PACKAGES	normal	enables querying any normal app on the device.	Allows query of any normal app on the device, regardless of manifest declarations.	
infosecadventures.allsafe.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference	

✓ ANDROID API

ok

ANDROID API

API	FILES
Local File I/O Operations	Show Files
Crypto	Show Files
Message Digest	Show Files
Loading Native Code (Shared Library)	Show Files
TCP Socket	Show Files
Starting Activity	Show Files
Inter Process Communication	Show Files
Starting Service	Show Files
Base64 Decode	Show Files
Dynamic Class and Dexloading	Show Files
Get Installed Applications	Show Files
WebView GET Request	Show Files
Get System Service	Show Files
Android Notifications	Show Files
Sending Broadcast	Show Files
Set or Read Clipboard data	Show Files
Java Reflection	Show Files
Execute OS Command	Show Files
Content Provider	Show Files

✓ NETWORK SECURITY

issue:- insecurely configured

NETWORK SECURITY

HIGH 1		WARNING 0		INFO 0		SECURE 0	
NO	SCOPE	SEVERITY	DESCRIPTION				
1	infosecadventures.io	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope				

✓ CERTIFICATE ANALYSIS











issue:- debug certificate used and sha256 and rsa collision

CERTIFICATE ANALYSIS

	HIGH 1	WARNING 2	INFO 1
TITLE	SEVERITY	DESCRIPTION	
Signed Application	info	Application is signed with a code signing certificate	
Application vulnerable to Janus Vulnerability	warning	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.	
Application signed with debug certificate	high	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.	
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.	





✓ MANIFEST ANALYSIS

issue:- debug enabled for android


Q MANIFEST ANALYSIS					
	HIGH 2	WARNING 7	INFO 0	SUPPRESSED 0	
NO	ISSUE	SEVERITY	DESCRIPTION		OPTIONS
1	App can be installed on a vulnerable unpatched Android version Android 6.0-6.0.1, [minSdk=23]	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	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.		
3	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.		
4	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.		
5	Activity (infosecadventures.allsafe.challenges.ProxyActivity) 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.		
6	Activity (infosecadventures.allsafe.challenges.DeepLinkTask) 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.		
7	Broadcast Receiver (infosecadventures.allsafe.challenges.NoteReceiver) is not Protected. [android:exported=true]	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.		
8	Service (infosecadventures.allsafe.challenges.RecorderService) is not Protected. [android:exported=true]	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.		
9	Content Provider (infosecadventures.allsafe.challenges.DataProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.		
10	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	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. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.		

✓ FIREBASE DATABASE ANALYSIS

issue:- firebase database analysis

FIREBASE DATABASE ANALYSIS		
   	Search: <input type="text"/>	
TITLE	SEVERITY	DESCRIPTION
Firestore Remote Config disabled	secure	Firestore Remote Config is disabled for https://firebase-remoteconfig.firebaseio.com/v1/projects/983632160629/namespaces/firebase-fetch?key=AtzaSyDjleCQ0-EikFb6vZIZmBfCSPNEYUck1g. This is indicated by the response: {"state": "NO_TEMPLATE"}
Open Firebase database	high	The Firebase database at https://allsafe-8cef0.firebaseio.com/.json is exposed to internet without any authentication

Showing 1 to 2 of 2 entries

Previous  Next

✓ POSSIBLE HARDCODED SECRETS

issue:- secret keys and api keys leaked

POSSIBLE HARDCODED SECRETS

Showing all 29 secrets

```
google_api_key": "Alza5y0JecQD-EkMBvZiZmBfCSPNEUYUcKlg"
key": "ebfb780-b2f6-41c6-bef3-4fba17be410c"
firebase_database_url": "https://allsafe-beef6.firebaseio.com"
google_crash_reporting_api_key": "Alza5y0JecQD-EkMBvZiZmBfCSPNEUYUcKlg"
c655a0670a04c0c93ecb62355b442c944139053fb521f628af60b4c3d8aa1405e77ef75928fe1dc127a2ffab6de3348b3c1856a429bf97e7e31c2e5bd66
1835a58E86ae668C48E6d3d32432C7f2e28f54b4
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
4fe342e2e1a7f9b8ee7eb4a7c0f9e162bce3357b0315ececbb6406837b5f1f5
258EAFAS-E914-47DA-95CA-CSAB0DC85B11
bc1q44ky6zalg27m45und3nprzt6rm9x9g2yc8
0a758729967eace3863a992c4f2b6ec29
1183929a789a3ba0045cd5f942c7d1bd99ef5440579b4a6817afbd17273a662c97ee72995ef42640c550b9013fa0761353c7086a272c24088be94769f016650
5ac35d8a3a3e7b3ebbd5576986bce551d06b0cc53b0f63bce3c3a27d2604b
3484cef7f6ff172c2cd78d3b51f3e66
6b17d1f2e124247f8bce6e563a40f277037d812deb33a0fa13945d898c296
6d2e1cdd505a108cc7e19a46aa30a8a
23456789abcdeghijklmnopqrstvwxyz
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b0b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451646b503f00
68647976001306097149819007990613932172694353001433054093944634591855431833976560521225596406614545549772963113914808508712198799710643812574026291115057151
11579208921035624876269744694940757353008614341529031419553363130867097853951
65dc4318c5e39c248c5b1c6e3534d
d51080eb22f8e684f1a19681eb7bdcf
6864797600130609714981900799061393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
3940206196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
11579208921035624876269744694940757352999695522413576034242259061068512044369
b3312fa7e23ee7e4988e056b3f82d19181d9c0efeb141120314088f5013875ac056396d8a2ed19d2a85c8ed3ec2aef
3940206196394479212279040100143613805079739270465446667946293404245721771496870329047266086258938001861060973112319
381744496232c05c0e9e9b92924c2996f41dbd289a147e9da3113b5f06b0c06a0b1ce1d7e819d7a43d1c90ee05f
212327297a7a5a743894a0e4a801f3
```

(B.) InsecureBankV2

Information

all basic info about application

APP SCORES

Security score

28/100

Trackers detected

3/432

MobileSF Scorecard

FILE INFORMATION

File name

InsecureBankv2.apk

Size

3.3 MB

MD5

5ee482906540f9c936ac861d1659f6

SHA1

80b5380a3cebfdf98311f5b26ccddc1bffa9b

SHA256

b18af2a0e44d7634bbcd93664d9c78a2695e050393cfbb5e8b91f902d193a8

APP INFORMATION

App Name

InsecureBankv2

Package Name

com.android.insecurebankv2

Main Activity

com.android.insecurebankv2.LoginActivity

Target SDK

22

Min SDK

15

Max SDK

Android Version Name

1.0

Android Version Code

1

4 / 10

EXPORTED ACTIVITIES

View All

0 / 0

EXPORTED SERVICES

View All

1 / 2

EXPORTED RECEIVERS

View All

1 / 1

EXPORTED PROVIDERS

View All

SIGNER CERTIFICATE

using only v1 certificate that not much secure

SIGNER CERTIFICATE

```
Binary is signed
v1 signature: True
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: C=MA, L=Boston, O=GI, OU=Services, CN=Dinesh Shetty
Signature Algorithm: rsaassa_pkcs1v15
Valid From: 2015-07-24 20:37:08+00:00
Valid To: 2040-07-17 20:37:08+00:00
Issuer: C=MA, L=Boston, O=GI, OU=Services, CN=Dinesh Shetty
Serial Number: 0x0bb4fe16
Hash Algorithm: sha256
md5: 6a736d89abb13d7165e7c7f909bac928d
sha1: k13be91a2b120f6c9dbb426e9f7c3b1e97741
sha256: 8902db81ae717486031a1534977de7f465ee112093e1553d38d41dffba0d57a375
sha512: 53770f3f69916f74dd6e750ae16fd9b23fa3b2c8e9e53b5a84262d7d7c44a26ede13e6db450abbcc1d9f64534802b8ebbb0b4de1da076b02112d9b122cbbd92
Found 1 unique certificates
```

APPLICATION PERMISSIONS

issue: unwanted permission as shown in ss

APPLICATION PERMISSIONS				
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_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.	
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.	
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.	
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.	
android.permission.READ_PROFILE	dangerous	read the user's personal profile data	Allows an application to read the user's personal profile data.	
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.	
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.	
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.	

✓ Trackers

some tracker tracking user

TRACKERS		
TRACKER NAME	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

Showing 1 to 3 of 3 entries

✓ CERTIFICATE ANALYSIS

issue:- application vulnerable to janus vulnerability

CERTIFICATE ANALYSIS		
HIGH 1	WARNING 0	INFO 1
TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	high	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-9.0, 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.
Signed Application	info	Application is signed with a code signing certificate

Showing 1 to 2 of 2 entries

Previous 1 Next

✓ MANIFEST ANALYSIS

issue:- multiple issues as shown in ss

MANIFEST ANALYSIS				
HIGH 6		WARNING 7		INFO 0
SUPPRESSED 0		Search: <input type="text"/>		
NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable unpatched Android version Android 4.0.3-4.0.4, [minSdk=15]	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=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.	
4	Activity (com.android.insecurebankv2.PostLogin) 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 (22) of the app to 29 or higher to fix this issue at platform level.	
5	Activity (com.android.insecurebankv2.PostLogin) 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.	
6	Activity (com.android.insecurebankv2.DoTransfer) 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 (22) of the app to 29 or higher to fix this issue at platform level.	
7	Activity (com.android.insecurebankv2.DoTransfer) 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 (com.android.insecurebankv2.ViewStatement) 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 (22) of the app to 29 or higher to fix this issue at platform level.	
9	Activity (com.android.insecurebankv2.ViewStatement) 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	Content Provider (com.android.insecurebankv2.TrackUserContentProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	

✓ POSSIBLE HARDCODED SECRETS

issue:- credentials are leaked

POSSIBLE HARDCODED SECRETS

▼ Showing all 25 secrets

"loginScreen_password": "Password:"
"loginScreen_username": "Username:"
EWZMQOzAsSbCW+73vnMc0IIA0IXmhdEPDWA4pBmTQF=

AK+A2i0KMMck37UYcOExFBrt2JDYu9ViuAHdYuT1VPLHst51ZSG89jehZq7ujXyH
2RUillTqy9QCgJa1LFspH1z+fWwdgPABYGujcpTf13CMmYA3W3Y+TBVqeDwkRNkY
w41pUAmD6TXdoU2/Z72GoKBjAyNw4B9JmpSTu2qFRaDsI7+5gLrSInCaebksSHto
Fych2TPIScbLJxRiDovUow7d3sVUDiaLAvtmgpW8g7e+3+ib/JMLjt3rF841gO
VECoKGIod10uMKpilFKK46zikIKVY7m5Sv4INe3KRY=
3oIDJEefykDk8VoOpv5sOi1YNQ0s4IEIre7qVmQXm2HQzIUqU6cNsaZxD6S8UMW
M/9MnPtadnnNpsJGLBqvtFaALLid0qI4JyMofQfSncPh=
KglVfxGq7C7ko+bqcJ8DTs8uzcctZAmLSX4/fuAvTk=
gcr/blkg3lQG930U0ghKqsUNHy1ZHgL5GjwbOVxLHrc=
6NX7jQU62u42sQ6Bcog9+pwW2loP1J/jqqDKEENUU4ZU=
eRIYZ7vwE2B0WWejblqyBziYzuBt9JW0243YOHXZvY=
Z17lzPChrfQy4VaYpiQxo0k7JJBJQR06QL2GGTFfGgU=
MU3VgnFcvu612xTEKnGZFJFowurNoeRHlUpl0GCgSFQ=
cs4+HqQNuLJCSjPmayUCJMLdoEEgnhD+nTAnE4ooENEnhW/TpxD13dq38SjFLmkW
qfDkyRZiTZGgubBz0juWMEqf8Qqw5CcMB2eo7wr2IH9X2v+qIFOYNd9v9fS1x0
4xZN7GqinxNwVj4iMqrRi7x6pRkbvrTHS+6N7nioqQ4QK45BALEp7Vftip3TGnlt
3mNwt4SZ3Etv5TihUa/RqoulNZPiat8RAS1ApJt5MxhvfIYxahkXg2hSNsePN+7M
PrVDFjRPs1s5jwZQRK3+ZFXo9PTI3zDMIRzLOPE43M8=
SxPdgyHHu8QFxBqcknBJfZgRiWxxWH3ut4/9iPAvil=
ir8bk+FXNtfVxQqTx81BUFTZKH1YNLABcK0MWI1xDng=
Y6D/YxZCnVSZsavLV5KYCoa8QyT30GvMdLessm7RE=
FaKwm3zfk+Dhq4JqMMBs2A+ODqwwgRuoVlqzQMyoaB4=

(C.) DVBA

✓ Information

all basic info about application

RECENT SCANSSTATIC ANALYZERDYNAMIC ANALYZERAPIDONATE▼DOCSABOUTSearch

APP SCORES

Security Score

44/100

Vulnerabilities

0/432

FILE INFORMATION

File Name

0x0a.apk

Size

3.61 MB

SHA1

2340b48cd80dbec30ba11432045b57ce

SHA256

23dc0688e4dd30c792309755a5b6d603df8789

SHA512

76c308facda655a353477177780e04feb1d91be032857768c891b2baf40bae

APP INFORMATION

App Name

DamnVulnerableBank

Package Name

com.app.damnVulnerableBank

Class Name

com.app.damnVulnerableBank.SplashScreen

Target SDK

29

Min SDK

21

Max SDK

Android version name

1.0

Android version Code

1

5 / 19

EXPORTED ACTIVITIES

View All

0 / 1

EXPORTED SERVICES

View All

0 / 0

EXPORTED RECEIVERS

View All

0 / 1

EXPORTED PROVIDERS

View All

SCAN OPTIONS

Manage Suppressions

Scan Logs

DECOMPILED CODE

✓ SIGNER CERTIFICATE

using only v2 certificate that not much secure

SIGNER CERTIFICATE

Binary is signed

v1 signature: False

v2 signature: True

v3 signature: False

v4 signature: None

x.509 Subject: o=Dvba, ou=Dvba, cn=damncorp

Signature Algorithm: rsaes-pkcs1v15

Valid From: 2020-10-29 07:43:13+00:00

Valid To: 2040-10-29 07:43:13+00:00

Issuer: o=Dvba, ou=Dvba, cn=damncorp

Serial Number: 0x1230704c

Hash Algorithm: sha256

md5: 41d437f06dc0f78901390b09341e540c8

sha1: e26ea75bdcab4769acedc4c78027aab8580a858

sha256: 0d770dd2df7f63e94e8ca87b7e97ba6827762e280bd281679910609568acdde

sha512: 0943f726cc5c543af6b72648ba2f628f56520870733622d2f615709af490e1b33174e7f18e349cce039e1d0303ab7e80fe47977ecce04ae28e01c0b9a6e0a58a5

Publickey Algorithm: rsa

Bit Size: 2048

Fingerprint: e9637ca3970bc7197333f1b6da9dd4ad5bb1fce7f1f123f1415751e103fda196

Found 1 unique certificates

✓ APPLICATION PERMISSIONS

all ok

APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.	Show Files
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.	Show Files
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.	Show Files

Showing 1 to 3 of 3 entries

Previous

1

Next

- ✓ ANDROID API

ANDROID API

Search:

API	FILES
Android Notifications	Show Files
Base64 Decode	Show Files
Base64 Encode	Show Files
Certificate Handling	Show Files
Crypto	Show Files
Dynamic Class and Dexloading	Show Files
Execute OS Command	Show Files
Get Installed Applications	Show Files
Get System Service	Show Files
GPS Location	Show Files

Showing 1 to 10 of 20 entries

Previous 1 2 Next

✓ NETWORK SECURITY

issue:- insecurely configured

NETWORK SECURITY

HIGH 2 WARNING 1 INFO 0 SECURE 0

Search:

NO	SCOPE	SEVERITY	DESCRIPTION
1		high	Base config is insecurely configured to permit clear text traffic to all domains.
2		high	Base config is configured to trust user installed certificates.
3	*	warning	Base config is configured to trust system certificates.

Showing 1 to 3 of 3 entries

Previous 1 Next

✓ CERTIFICATE ANALYSIS

ok

CERTIFICATE ANALYSIS

HIGH 0 WARNING 0 INFO 1

Search:

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

Showing 1 to 1 of 1 entries

Previous 1 Next

✓ MANIFEST ANALYSIS

issue:- multiple issues as shown in ss

MANIFEST ANALYSIS

HIGH4

WARNING6

INFO0

SUPPRESSED0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable unpatched Android version [android:usesCleartextTraffic=true]	High	This application can be installed on an older version of android that has multiple unfixd vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.	<div></div>
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	High	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.	<div></div>
3	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	Info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.	<div></div>
4	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.	<div></div>
5	App Link assetlinks.json file not found [android:name=com.app.damnvulnerablebank.CurrencyRates] [android:host=http://we.com]	High	App Link asset verification URL (http://we.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PIN, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.	<div></div>
6	App Link assetlinks.json file not found [android:name=com.app.damnvulnerablebank.CurrencyRates] [android:host=https://we.com]	High	App Link asset verification URL (https://we.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PIN, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.	<div></div>
7	Activity (com.app.damnvulnerablebank.CurrencyRates) 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.	<div></div>
8	Activity (com.app.damnvulnerablebank.SendMoney) 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.	<div></div>
9	Activity (com.app.damnvulnerablebank.ViewBalance) 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.	<div></div>
10	Activity (androidx.biometric.DeviceCredentialHandlerActivity) 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.	<div></div>

✓ FIREBASE DATABASE ANALYSIS

ok

FIREBASE DATABASE ANALYSIS		
Search: <input type="text"/>		
TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	Info	The app talks to Firebase database at https://damnvulnerable-bank.firebaseio.com
Firebase Remote Config disabled	Secure	Firebase Remote Config is disabled for https://firebase-remoteconfig.googleapis.com/v1/projects/932398433474/namespaces/firebase:fetch?key=AlzaSyBbOHG6DDa6DOcRGeg57mw9nXYXcw6la3c. This is indicated by the response: {"state": "NO_TEMPLATE"}

✓ POSSIBLE HARDCODED SECRETS

✓ issue:- api key leaked

POSSIBLE HARDCODED SECRETS	
Showing all 4 secrets	
"google_api_key" : "AlzaSyBbOHG6DDa6DOcRGeg57mw9nXYXcw6la3c"	
"firebase_database_url" : "https://damnvulnerable-bank.firebaseio.com"	
"google_crash_reporting_api_key" : "AlzaSyBbOHG6DDa6DOcRGeg57mw9nXYXcw6la3c"	
GmdBWksdEwAZFAILLVEDx1FKS0JtQ1DhGgaBkNXQQFjTkdBTUMJBgMCFQUIFA5MXUFPDxUdBg4PckNwY05HQU1DFAYaDwgDBlhTTkUSAgwFHQcJBk9rWkkTbRw=	

2. Static Analysis of iOS App

(A.) iGoat

✓ Information

all basic info about application

The screenshot shows the MobSF application overview page. It features a top navigation bar with links for RECENT SCANS, STATIC ANALYZER, DYNAMIC ANALYZER, API, DONATE, DOCS, and ABOUT. The main content area is divided into four sections: APP SCORES, FILE INFORMATION, APP INFORMATION, and BINARY INFORMATION. The APP SCORES section shows a Security Score of 52/100 and a Trackers Detection of 0/432. The FILE INFORMATION section lists the file name as iGoat-Swift.ipa, size as 15.33MB, MD5 as 473a7b648e090a445f6bc06253a2ae60, SHA1 as e560f0633d96a40f1d0f949f3a854830e3af50, and SHA256 as 364273106c7f6b7b627b7f821a1539af4044025b7f190ebb760afb4b85c15a47. The APP INFORMATION section lists the app name as iGoat-Swift, app type as Swift, identifier as QWASPIGoat-Swift, SDK name as iPhoneOS13.2, version as 1.0, build as 1, platform version as 13.2, min OS version as 10.0, and supported platforms as iPhoneOS. The BINARY INFORMATION section lists the arch as ARM, cpu_subtype as CPU_SUBTYPE_ARM_V7, and bit as 32-bit. Below these sections are two tabs: SCAN OPTIONS and DECOMPILED ASSETS. The SCAN OPTIONS tab has buttons for Rescan, Manage Suppressions, and Scan Log. The DECOMPILED ASSETS tab has buttons for View Info.plist, View Class Dump, and Download IPA.

✓ ATS

issue: App Transport Security AllowsArbitraryLoads is allowed

The screenshot shows the MobSF App Transport Security (ATS) section. It features a top navigation bar with links for RECENT SCANS, STATIC ANALYZER, DYNAMIC ANALYZER, API, DONATE, DOCS, and ABOUT. The main content area is divided into four sections: APP SCORES, FILE INFORMATION, APP INFORMATION, and BINARY INFORMATION. The APP SCORES section shows a Security Score of 52/100 and a Trackers Detection of 0/432. The FILE INFORMATION section lists the file name as iGoat-Swift.ipa, size as 15.33MB, MD5 as 473a7b648e090a445f6bc06253a2ae60, SHA1 as e560f0633d96a40f1d0f949f3a854830e3af50, and SHA256 as 364273106c7f6b7b627b7f821a1539af4044025b7f190ebb760afb4b85c15a47. The APP INFORMATION section lists the app name as iGoat-Swift, app type as Swift, identifier as QWASPIGoat-Swift, SDK name as iPhoneOS13.2, version as 1.0, build as 1, platform version as 13.2, min OS version as 10.0, and supported platforms as iPhoneOS. The BINARY INFORMATION section lists the arch as ARM, cpu_subtype as CPU_SUBTYPE_ARM_V7, and bit as 32-bit. Below these sections are two tabs: SCAN OPTIONS and DECOMPILED ASSETS. The SCAN OPTIONS tab has buttons for Rescan, Manage Suppressions, and Scan Log. The DECOMPILED ASSETS tab has buttons for View Info.plist, View Class Dump, and Download IPA.

✓ APPLICATION PERMISSIONS

ok

The screenshot shows the MobSF Application Permissions section. It features a top navigation bar with links for RECENT SCANS, STATIC ANALYZER, DYNAMIC ANALYZER, API, DONATE, DOCS, and ABOUT. The main content area is divided into four sections: APP SCORES, FILE INFORMATION, APP INFORMATION, and BINARY INFORMATION. The APP SCORES section shows a Security Score of 52/100 and a Trackers Detection of 0/432. The FILE INFORMATION section lists the file name as iGoat-Swift.ipa, size as 15.33MB, MD5 as 473a7b648e090a445f6bc06253a2ae60, SHA1 as e560f0633d96a40f1d0f949f3a854830e3af50, and SHA256 as 364273106c7f6b7b627b7f821a1539af4044025b7f190ebb760afb4b85c15a47. The APP INFORMATION section lists the app name as iGoat-Swift, app type as Swift, identifier as QWASPIGoat-Swift, SDK name as iPhoneOS13.2, version as 1.0, build as 1, platform version as 13.2, min OS version as 10.0, and supported platforms as iPhoneOS. The BINARY INFORMATION section lists the arch as ARM, cpu_subtype as CPU_SUBTYPE_ARM_V7, and bit as 32-bit. Below these sections are two tabs: SCAN OPTIONS and DECOMPILED ASSETS. The SCAN OPTIONS tab has buttons for Rescan, Manage Suppressions, and Scan Log. The DECOMPILED ASSETS tab has buttons for View Info.plist, View Class Dump, and Download IPA.

✓ BINARY CODE ANALYSIS

issue:-

1. Binary makes use of insecure API(s)
2. Binary makes use of the insecure Random function(s)

IPA BINARY CODE ANALYSIS

HIGH0

WARNING3

INFO2

SECURE0

SUPPRESSED0

Search:

NO	ISSUE	SEVERITY	STANDARDS	DESCRIPTION	OPTIONS
1	Binary makes use of Insecure API(s)	Warning	CWE: CWE-676: Use of Potentially Dangerous Function OWASP Top 10: M7: Client Code Quality OWASP MASVS: MSGT-CODE-8	The binary may contain the following insecure API(s) : fopen , memcpy , strcpy , strlen , strcmp	<div></div>
2	Binary makes use of the insecure Random function(s)	Warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSGT-CRYPTO-4	The binary may use the following insecure Random function(s) : random	<div></div>
3	Binary makes use of Logging function	Info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSGT-STORAGE-3	The binary may use _NSLog function for logging.	<div></div>
4	Binary makes use of malloc function	Warning	CWE: CWE-789: Uncontrolled Memory Allocation OWASP Top 10: M7: Client Code Quality OWASP MASVS: MSGT-CODE-8	The binary may use _malloc function instead of calloc	<div></div>
5	Binary uses WebView Component.	Info	OWASP MASVS: MSGT-CODE-9	The binary may use UIWebView Component.	<div></div>

Showing 1 to 5 of 5 entries

Showing 1 to 5 of 5 entries

✓ FRAMEWORK BINARY ANALYSIS

issues:- many issue as shown in ss

DYNAMIC LIBRARY & FRAMEWORK BINARY ANALYSIS								
Search:								
NO	DYLIB/Framework	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
1	Frameworks/libswiftFoundation.dylib	False The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	True This binary has a stack canary value added to the stack so that it will be overwritten by a code buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	True The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.	False The binary does not have Rpath Search Path (@rpath) set.	True This binary has a code signature.	False This binary is not encrypted.	False Debug Symbols are available. To strip debugging symbols, set Strip Debug Symbols During Copy to YES, Deployment Postprocessing to YES, and Strip Linked Product to YES in project's build settings.
2	Frameworks/libswiftObjectiveC.dylib	False The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	False This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. This might be okay for pure Swift dylibs.	False The binary is not compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and protects from memory corruption vulnerabilities. Use compiler option -fobjc-arc to enable ARC or set Objective-C Automatic Reference Counting to YES in project configuration.	False The binary does not have Rpath Search Path (@rpath) set.	True This binary has a code signature.	False This binary is not encrypted.	False Debug Symbols are available. To strip debugging symbols, set Strip Debug Symbols During Copy to YES, Deployment Postprocessing to YES, and Strip Linked Product to YES in project's build settings.
3	Frameworks/libswiftCoreFoundation.dylib	False The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	False This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. This might be okay for pure Swift dylibs.	False The binary is not compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and protects from memory corruption vulnerabilities. Use compiler option -fobjc-arc to enable ARC or set Objective-C Automatic Reference Counting to YES in project configuration.	False The binary does not have Rpath Search Path (@rpath) set.	True This binary has a code signature.	False This binary is not encrypted.	False Debug Symbols are available. To strip debugging symbols, set Strip Debug Symbols During Copy to YES, Deployment Postprocessing to YES, and Strip Linked Product to YES in project's build settings.
4	Frameworks/libswiftCoreImage.dylib	False The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	False This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. This might be okay for pure Swift dylibs.	False The binary is not compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and protects from memory corruption vulnerabilities. Use compiler option -fobjc-arc to enable ARC or set Objective-C Automatic Reference Counting to YES in project configuration.	False The binary does not have Rpath Search Path (@rpath) set.	True This binary has a code signature.	False This binary is not encrypted.	False Debug Symbols are available. To strip debugging symbols, set Strip Debug Symbols During Copy to YES, Deployment Postprocessing to YES, and Strip Linked Product to YES in project's build settings.

✓ POSSIBLE HARDCODED SECRETS

issue:- user password leaked

