Assignment 6 – Static Analysis (Android & iOS)

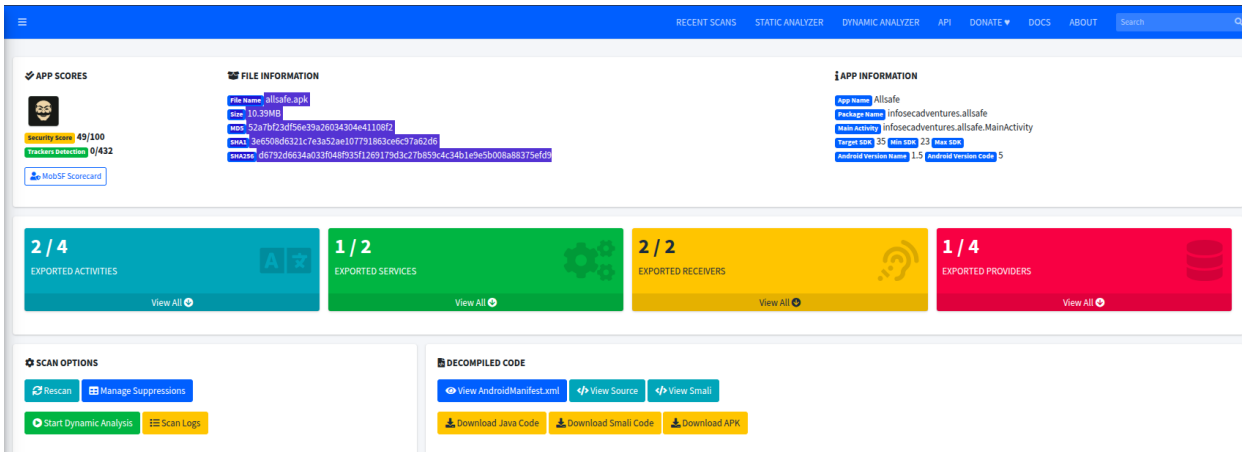
---

1. Static Analysis of Android App

(A.) Allsafe

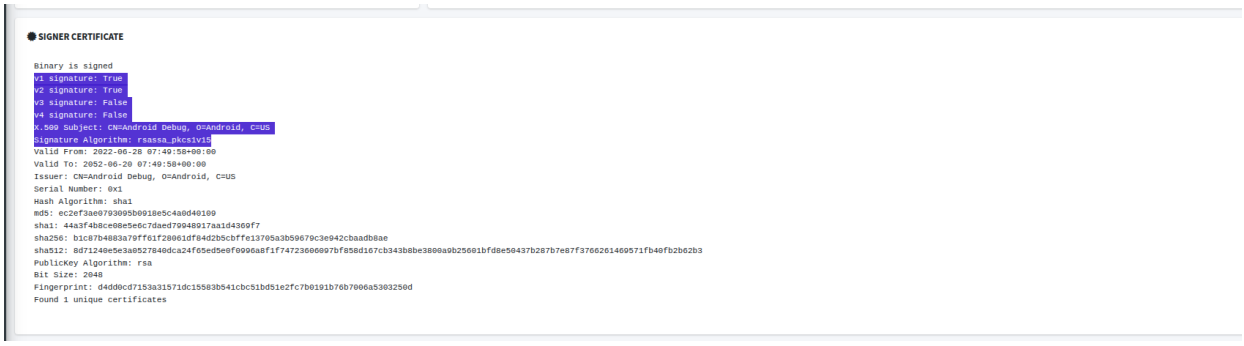
- ✔ Information

  all basic info about application



- ✔ SIGNER CERTIFICATE

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



- ✔ 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	WARNING	INFO	SECURE
1	0	0	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	WARNING	INFO
1	2	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

MANIFEST ANALYSIS

HIGH	WARNING	INFO	SUPPRESSED
2	7	0	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.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:

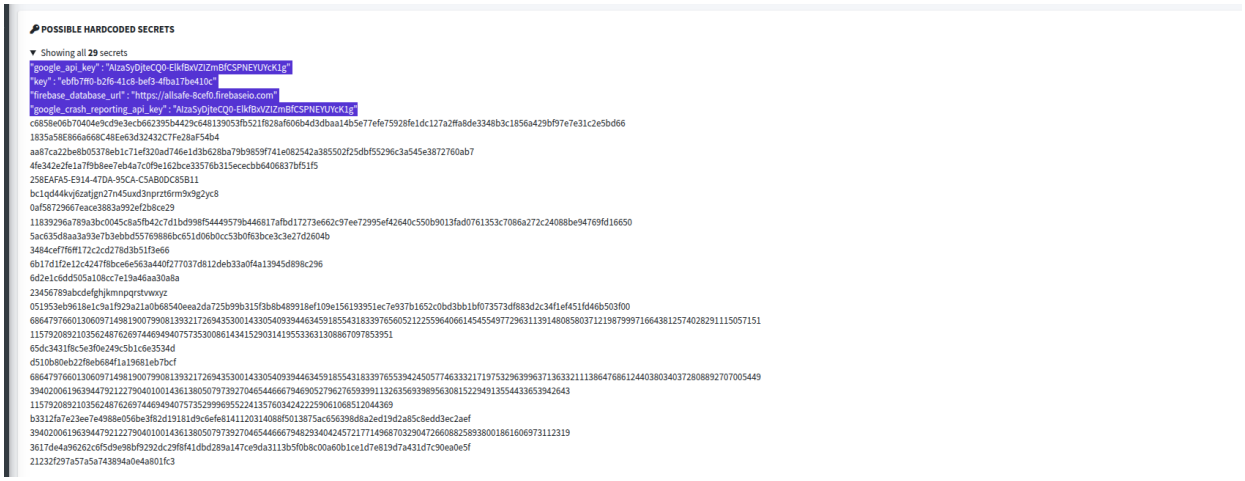
TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/983632160629/namespaces/firebase:fetch?key=AIzaSyDjteCQ0-ElkfBxVZIZmBfCSPNEYUYcK1g. This is indicated by the response: {'state': 'NO_TEMPLATE'}
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 1 Next

✔ POSSIBLE HARDCODED SECRETS

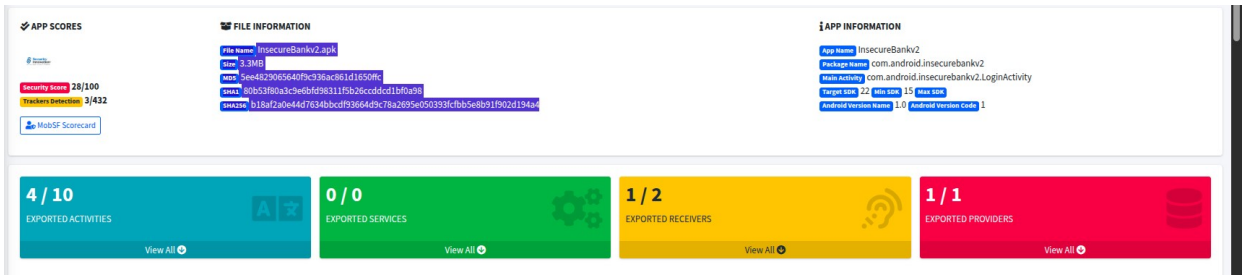
issue:- secret keys and api keys leaked



(B.) InsecureBankV2

- ✔ Information

  all basic info about application



- ✔ SIGNER CERTIFICATE

  using only v1 certificate that not much secure

- ✔ APPLICATION PERMISSIONS

  issue: unwanted permission as shown in ss

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_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

Search:

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.
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	WARNING	INFO	SUPPRESSED
6	7	0	0

Search:

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

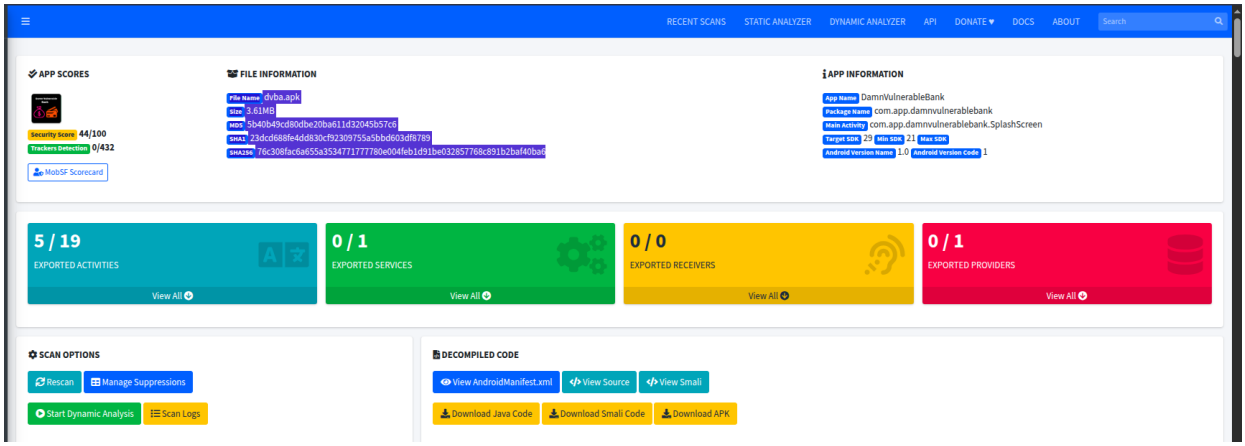
▼ Showing all **25** secrets

"loginscreen_password" : "Password:"
"loginscreen_username" : "Username:"
EwZMQOzAsSbCW+73vnMc0IlAOIXmhdEPDWA4pBmTQFs=
AK+A2I0KMMcK37UYcOExFBrt2JDYu9VIuAHdYuT1VPLHst51ZSG89jehZq7ujXyH
2RUillTqy9QCgJa1LFspH1z+fWwdgPAByGujcpTf13CMmYA3W3Y+TBVqeDwkRNkY
w41pUAmd6TXdoU2/Z72GoKBjAyNw4B9JmpSTu2qFRaDsI7+5gLrSInCAebksSHto
Fych2TPIScbLJxRIDoDvUow7d3sVUDiaLAvtmgpWr8g7e+3+ib/JMLjt3rf841gO
VECoKGlOd10uMKpiLFkK46zikCIkVy7m5Sv4INe3KRY=
3oIDJEetfykDk8YoOpv5sOi1YNQ0s4lEIre7qVmQXm2HQzlUqU6cNsaZxD6S8UMW
M/9MnPtaDnNpsJGLBqvtFaALld0ql4JyMOfQfSncPhI=
KglVFfxGq7C7ko+bqcJ8DTs8uzcctZAmlSX4/fuAvTk=
gcr/blkg3lQG930U0ghKqsUNHy1ZHgL5GjwbOVxLHrc=
6NX7jQU62u42sQ6Bcog9+pwW2loP1J/qqDKEENUU4ZU=
eRIYZ7vwE2B0WWejblqyBziYzuBt9JW024X3YOHX2vY=
Z17lzPChrfQy4VaYpiQXo0k7JJBjQR06QL2GGTFiGqU=
MU3VGnFcvu612xTEKnGZFJFOwurNoeRHlUpI0GCgSFQ=
cs4+HQqNuLJCSjPmayUCjMLdoEEgnhD+nTAnE4ooENEnhW/TpxD13dq38SjFLmkW
qfDkyRZiTZGguvBzojuWMEqfl8Qqw5CcMB2eo7wr2iH9X2v+qlFOYNd9v9ffS1x0
4xZN7GqinxNwVj4iMqrRi7x6pRkbvrTHS+6N7nioqQ4QK45BALEp7VFtIp3TGnIt
3mNwt4SZ3Etv5TlhUa/RqouLnZPiat8RAS1ApJt5MxhvfIYxahkXg2hSNsePN+7M
PrVDFjRPs1s5jwZQRK3+ZFXo9PTi3zDMlRzL0PE43M8=
SxPdgyHHu8QFxBqcknBJfZgRiWxxWH3utf4/9iPAvil=
ir8bk+FXNtfVxQqTx81BUFTZKH1YNLABcK0MWl1xDng=
Y6D/YxzOCnVSZVsavLV5KYCoa8QyT30GvMdLessm7RE=
FaKwm3zfk+Dhq4JqMMBs2A+ODqwwgRuoVlqzQMyOaB4=

(C.) DVBA

✔ Information

all basic info about application

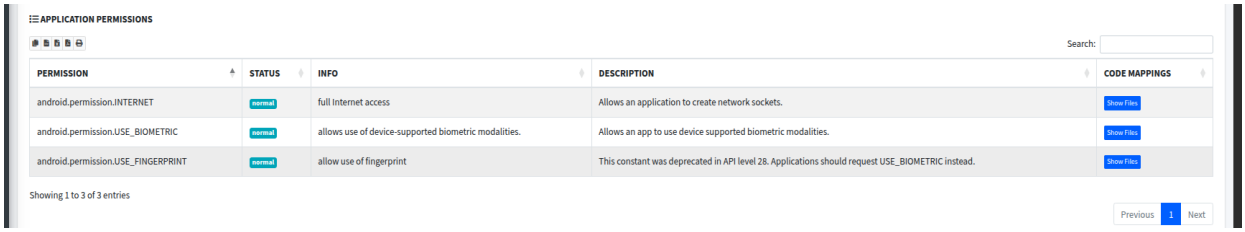


✔ SIGNER CERTIFICATE

using only v2 certificate that not much secure

✔ APPLICATION PERMISSIONS

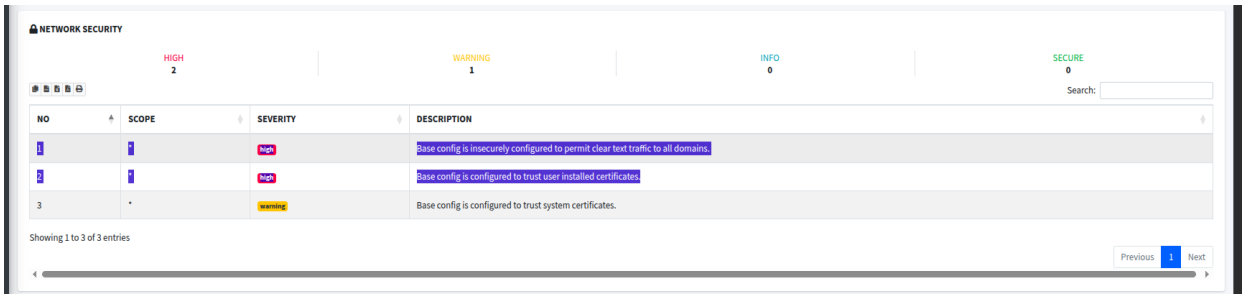
all ok



✔ ANDROID API

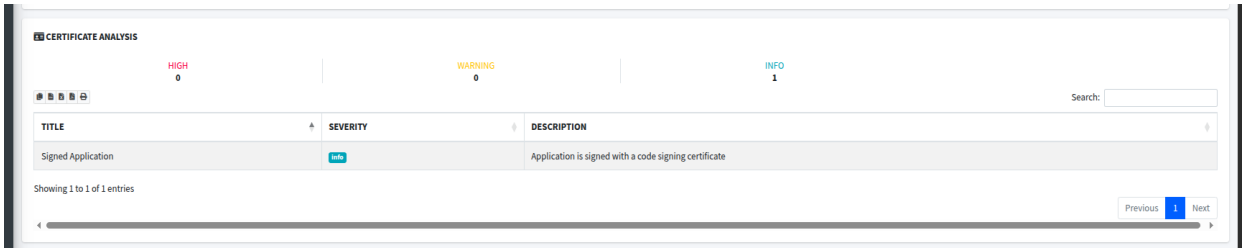
✔ NETWORK SECURITY

issue:- insecurely configured



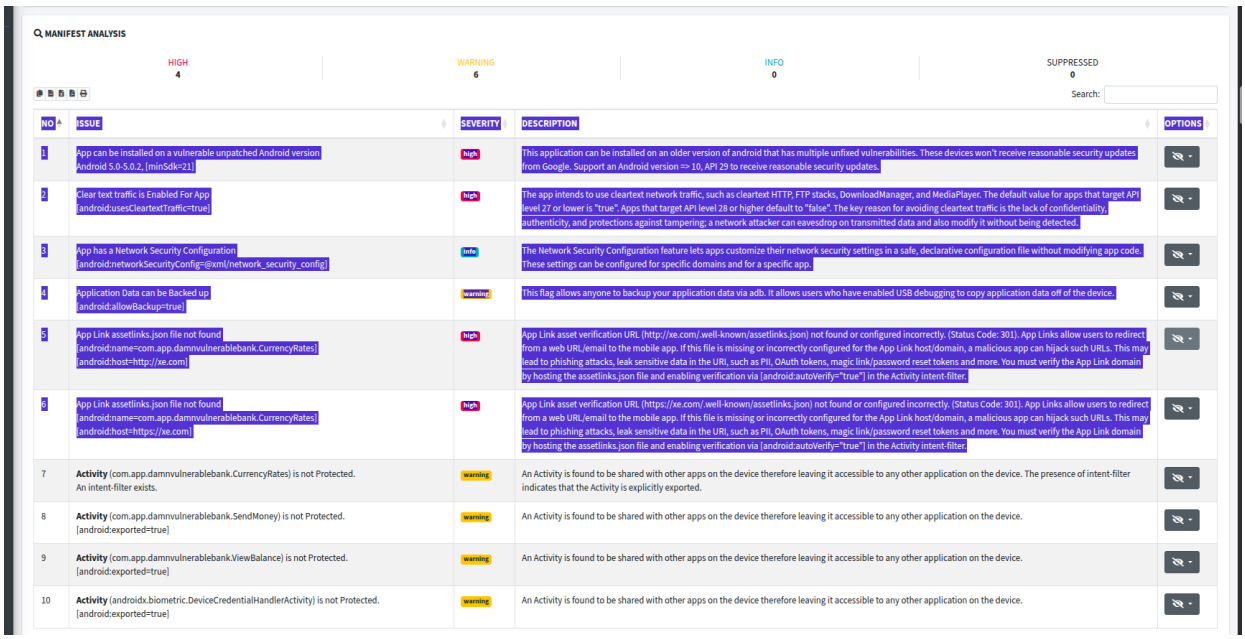
✔ CERTIFICATE ANALYSIS

ok



✔ MANIFEST ANALYSIS

issue:- multiple issues as shown in ss



MANIFEST ANALYSIS

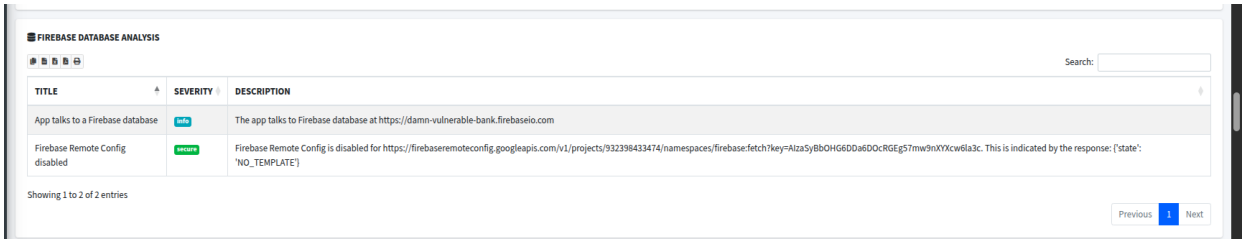
HIGH	WARNING	INFO	SUPPRESSED
4	6	0	0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable unpatched Android version Android 5.0-5.0.2, [minSdk=21]	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	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.	
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.	
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	App Link assetlinks.json file not found [android:name=com.app.damnvulnerablebank.CurrencyRates] [android:host=http://xe.com]	high	App Link asset verification URL (http://xe.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 PII, 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.	
6	App Link assetlinks.json file not found [android:name=com.app.damnvulnerablebank.CurrencyRates] [android:host=https://xe.com]	high	App Link asset verification URL (https://xe.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 PII, 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.	
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.	
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.	
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.	
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.	

- ✔ FIREBASE DATABASE ANALYSIS

  ok



FIREBASE DATABASE ANALYSIS

Search:

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://damn-vulnerable-bank.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/932398433474/namespaces/firebase:fetch?key=AIzaSyBbOHG6DDa6DOcRGEg57mw9nXYXcw6la3c. This is indicated by the response: {'state': 'NO_TEMPLATE'}

Showing 1 to 2 of 2 entries

Previous 1 Next

- ✔ POSSIBLE HARDCODED SECRETS
- ✔ issue:- api key leaked

POSSIBLE HARDCODED SECRETS

▼ Showing all 4 secrets

"google_api_key" : "AIzaSyBbOHG6DDa6DOcRGEg57mw9nXYXcw6la3c"

"firebase_database_url" : "https://damn-vulnerable-bank.firebaseio.com"

"google_crash_reporting_api_key" : "AIzaSyBbOHG6DDa6DOcRGEg57mw9nXYXcw6la3c"

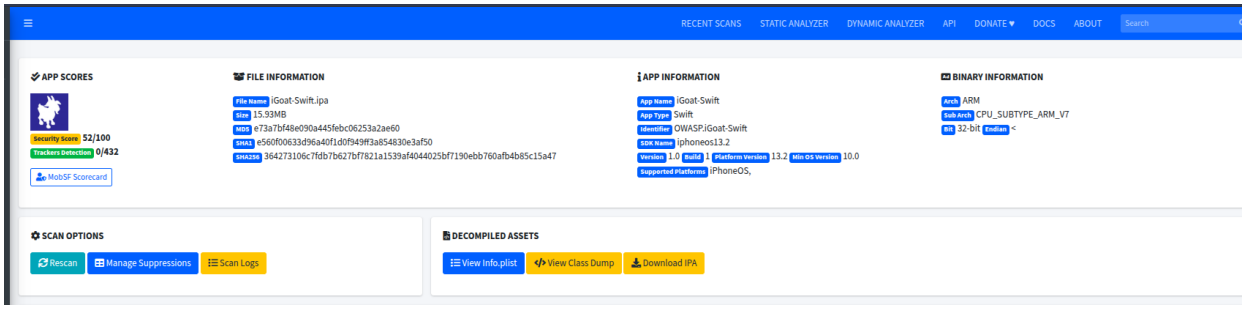
GmdBWksdEwAZFAlLVEdDX1FKS0JtQU1DHggaBkNXQQFjTkdBTUMJBgMCFQUIFA5MXUFPDxUdBg4PCkNWY05HQU1DFAYaDwgDBlhTTkUSAgwfHQcJBk9rWkkTbRw=

2. Static Analysis of iOS App

(A.) iGoat

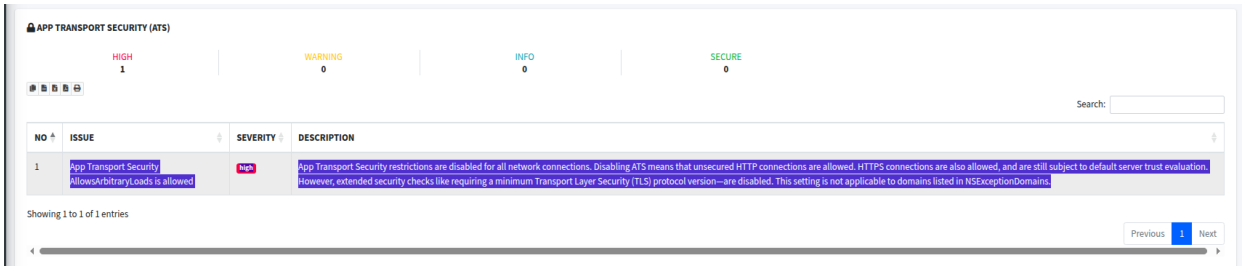
- ✔ Information

all basic info about application



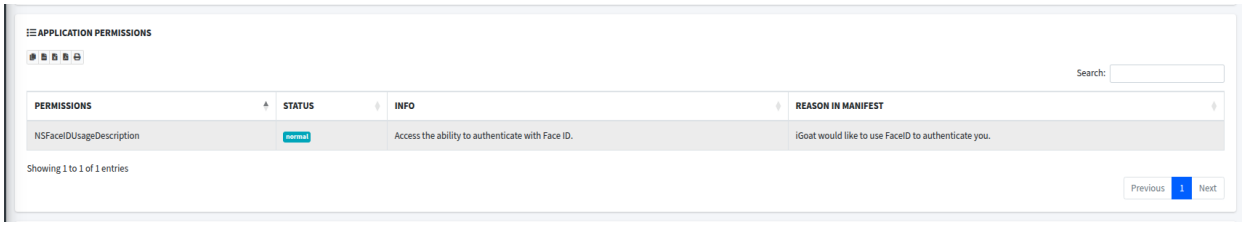
✔ ATS

issue: App Transport Security AllowsArbitraryLoads is allowed



✔ APPLICATION PERMISSIONS

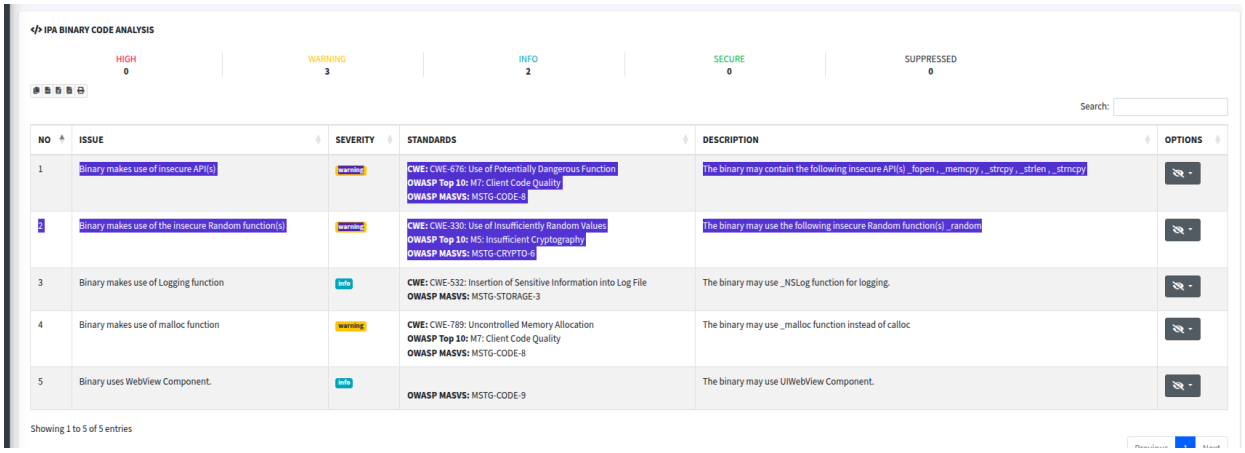
ok



✔ 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

HIGH	WARNING	INFO	SECURE	SUPPRESSED
0	3	2	0	0

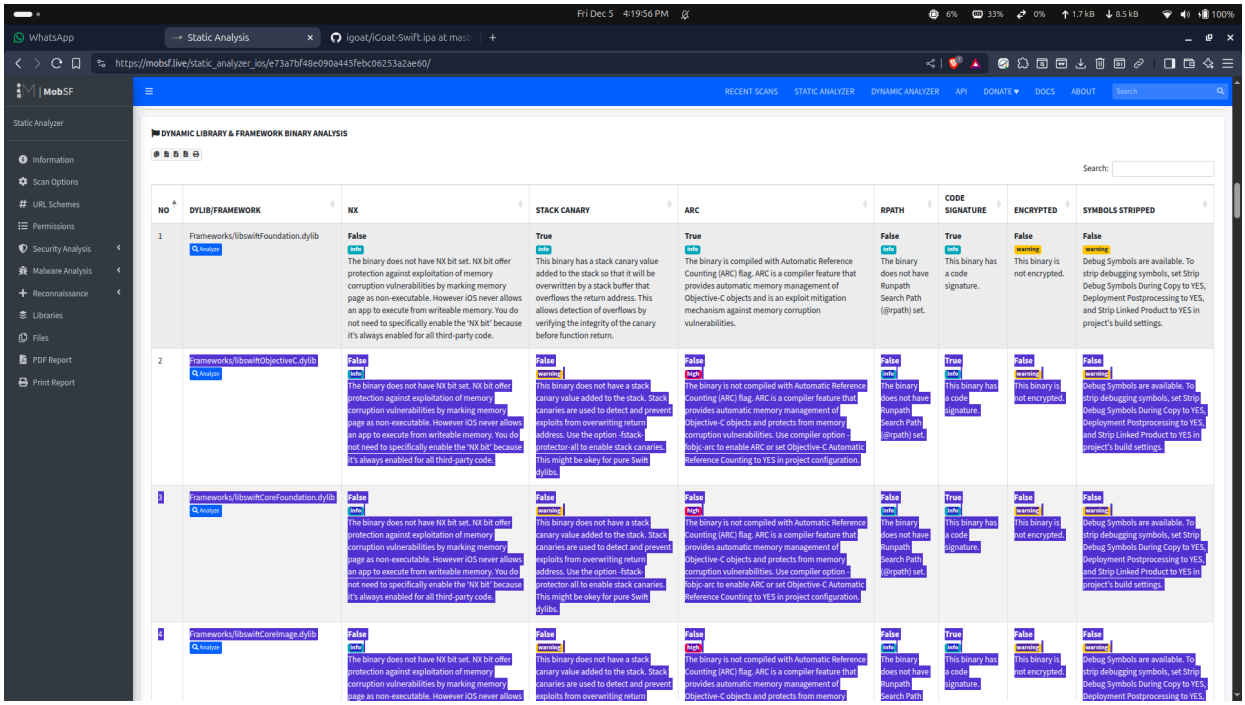
Search:

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:** MSTG-CODE-8	The binary may contain the following insecure API(s) _fopen , _memcpy , _strcpy , _strlen , _strncpy	
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:** MSTG-CRYPTO-6	The binary may use the following insecure Random function(s) _random	
3	Binary makes use of Logging function	info	**CWE:** CWE-532: Insertion of Sensitive Information into Log File **OWASP MASVS:** MSTG-STORAGE-3	The binary may use _NSLog function for logging.	
4	Binary makes use of malloc function	warning	**CWE:** CWE-789: Uncontrolled Memory Allocation **OWASP Top 10:** M7: Client Code Quality **OWASP MASVS:** MSTG-CODE-8	The binary may use _malloc function instead of calloc	
5	Binary uses WebView Component.	info	**OWASP MASVS:** MSTG-CODE-9	The binary may use UIWebView Component.	

Showing 1 to 5 of 5 entries

✔ FRAMEWORK BINARY ANALYSIS

issues:- many issue as shown in ss

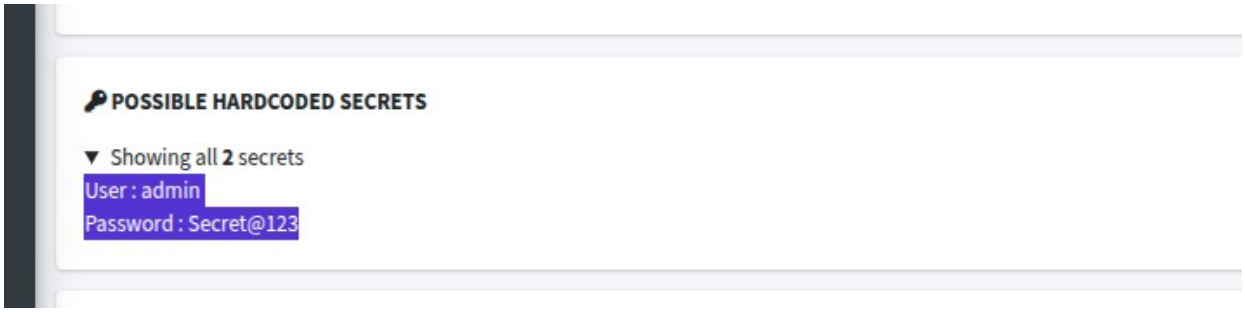


DYNAMIC LIBRARY & FRAMEWORK BINARY ANALYSIS

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 writeable 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 stack 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 Runpath 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 writeable 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 okey 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 Runpath 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 writeable 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 okey 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 Runpath 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	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	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	False The binary does not have Runpath Search Path	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.

✔ POSSIBLE HARDCODED SECRETS

issue:- user password leaked



POSSIBLE HARDCODED SECRETS

▼ Showing all 2 secrets

User : admin

Password : Secret@123