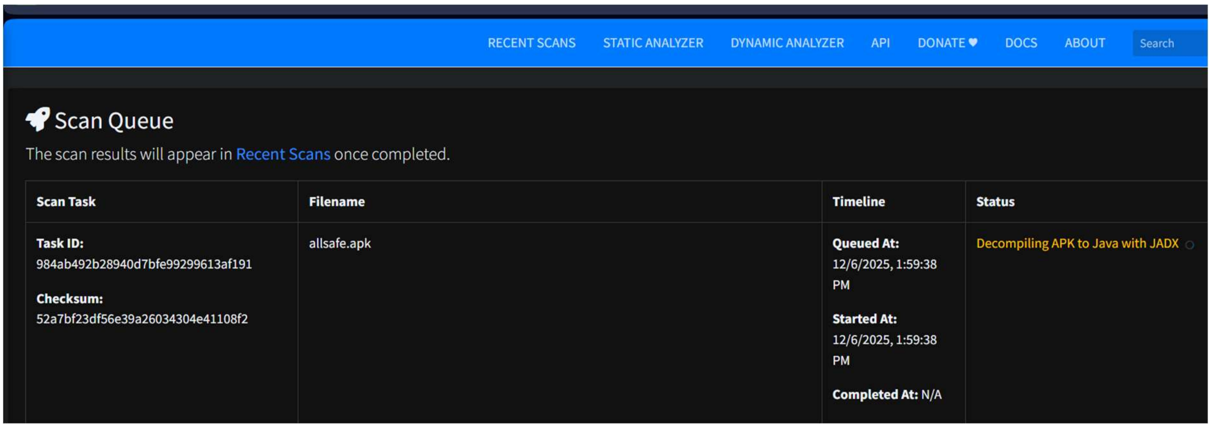
Assignment 6 - Static Analysis of Android & IOS

1)Using app Allsafe.apk

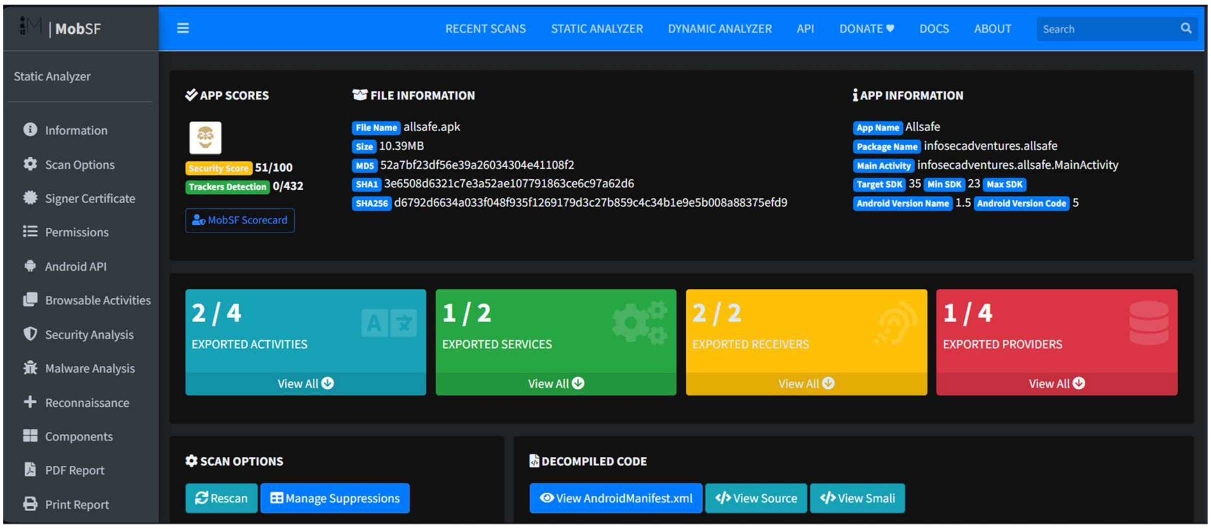


Scan Queue

The scan results will appear in Recent Scans once completed.

Scan Task	Filename	Timeline	Status
Task ID: 984ab492b28940d7bfe99299613af191 **Checksum:** 52a7bf23df56e39a26034304e41108f2	allsafe.apk	**Queued At:** 12/6/2025, 1:59:38 PM **Started At:** 12/6/2025, 1:59:38 PM **Completed At:** N/A	Decompiling APK to Java with JADX

Files Hash info exist



APP SCORES

Security Score 51/100
Trackers Detection 0/432

FILE INFORMATION

File Name allsafe.apk
Size 10.39MB
MD5 52a7bf23df56e39a26034304e41108f2
SHA1 3e6508d6321c7e3a52ae107791863ce6c97a62d6
SHA256 d6792d6634a033f048f935f1269179d3c27b859c4c34b1e9e5b008a88375efd9

APP INFORMATION

App Name Allsafe
Package Name infosecadventures.allsafe
Main Activity infosecadventures.allsafe.MainActivity
Target SDK 35 Min SDK 23 Max SDK
Android Version Name 1.5 Android Version Code 5

2 / 4 EXPORTED ACTIVITIES

1 / 2 EXPORTED SERVICES

2 / 2 EXPORTED RECEIVERS

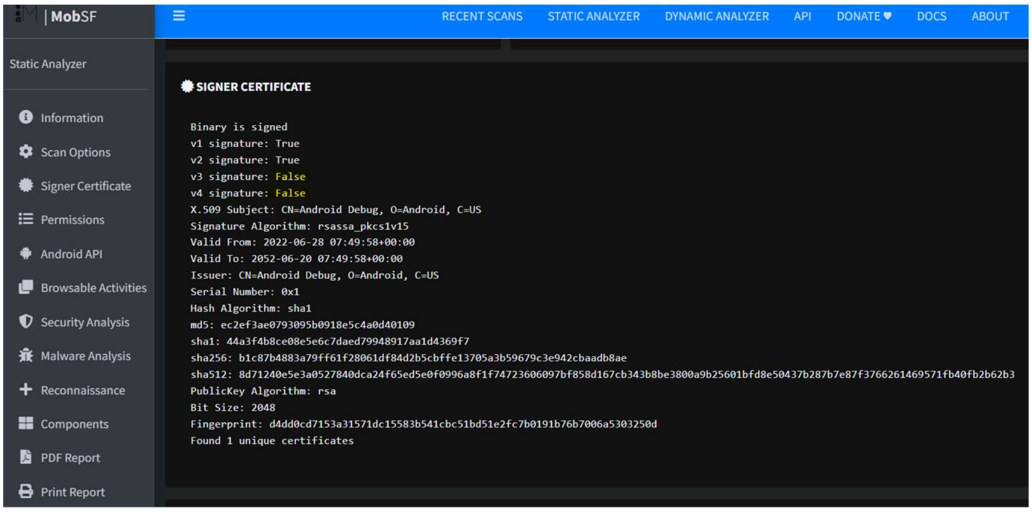
1 / 4 EXPORTED PROVIDERS

SCAN OPTIONS

DECOMPILED CODE

Signer certificate

Problem-: No v3 and v4 signature available

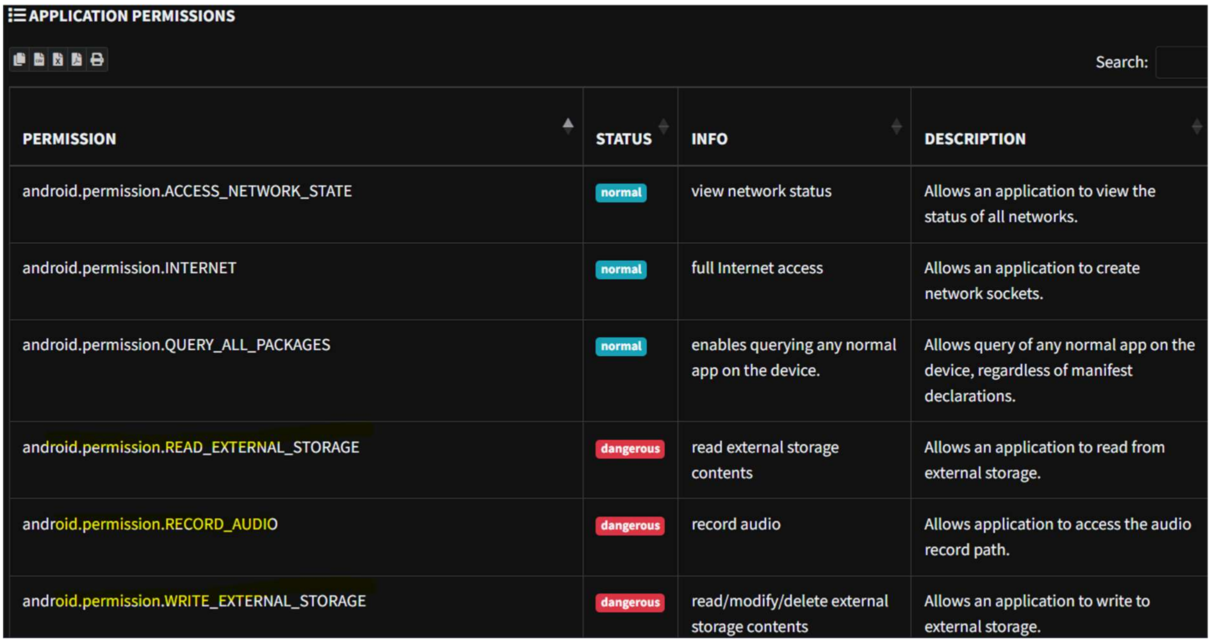


SIGNER CERTIFICATE

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: CN=Android Debug, O=Android, C=US
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-06-28 07:49:58+00:00
Valid To: 2052-06-20 07:49:58+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha1
md5: ec2ef3ae0793095b0918e5c4a0d40109
sha1: 44a3f4b8ce08e5e6c7daed79948917aa1d4369f7
sha256: b1c87b4883a79ff61f28061df84d2b5cbffe13705a3b59679c3e942cbaadb8ae
sha512: 8d71240e5e3a0527840dca24f65ed5e0f0996a8f1f74723606097bf858d167cb343b8be3800a9b25601bfd8e50437b287b7e87f3766261469571fb40fb2b62b3
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: d4dd0cd7153a31571dc15583b541cbc51bd51e2fc7b0191b76b7006a5303250d
Found 1 unique certificates
```

Application permissions

Problem-: Dangerous permission required

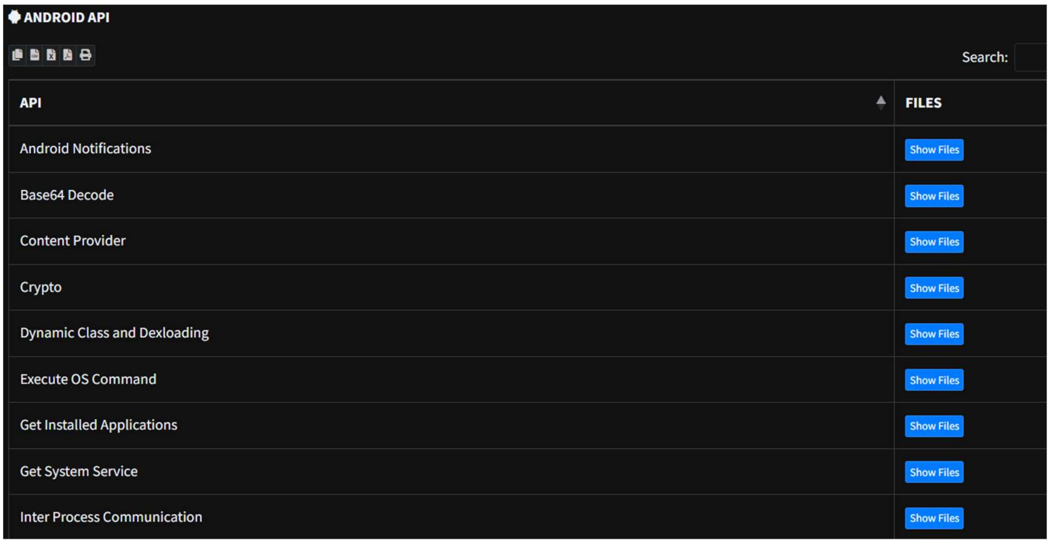


APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

Android API – No Problem exist

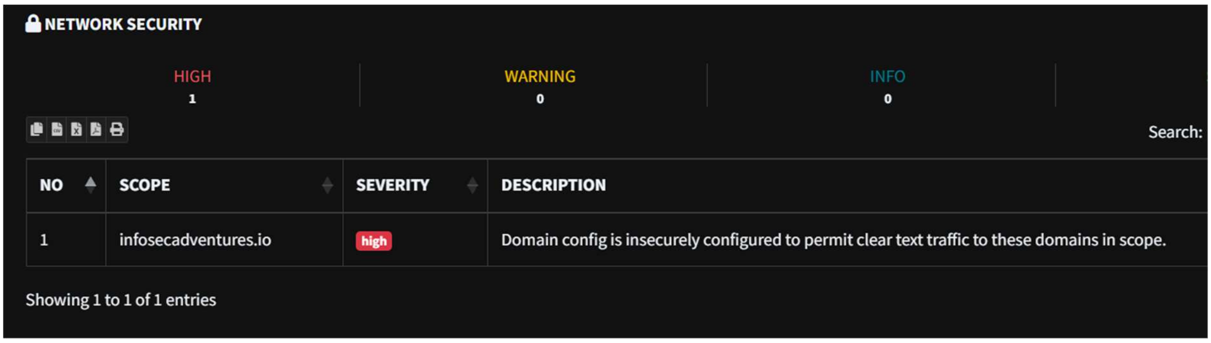


ANDROID API

Search:

API	FILES
Android Notifications	Show Files
Base64 Decode	Show Files
Content Provider	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
Inter Process Communication	Show Files

Network Security- Not secure



NETWORK SECURITY

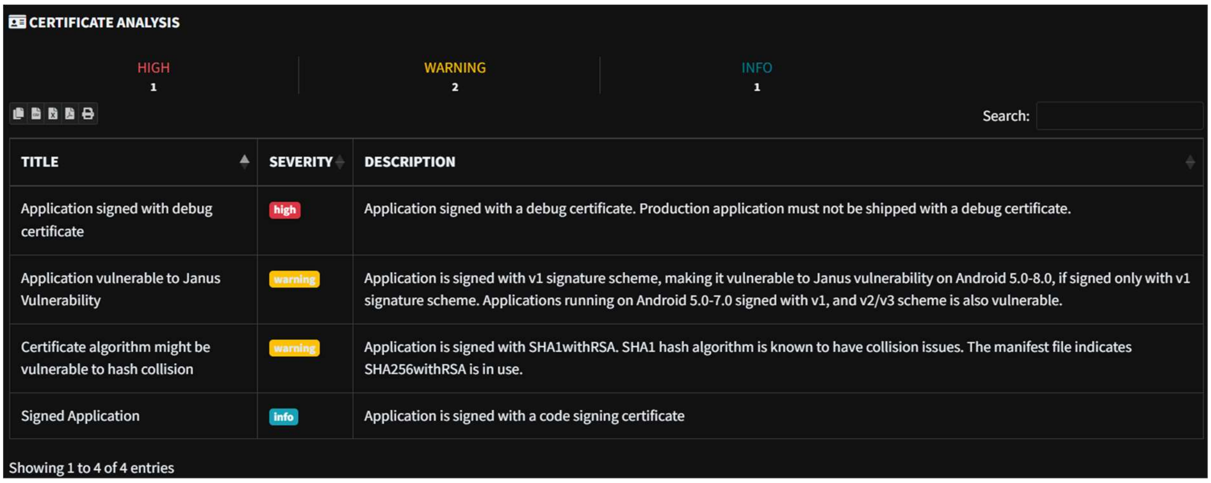
HIGH	WARNING	INFO
1	0	0

Search:

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

Showing 1 to 1 of 1 entries

Certificate Analysis- Issue exist



CERTIFICATE ANALYSIS

HIGH 1 | WARNING 2 | INFO 1

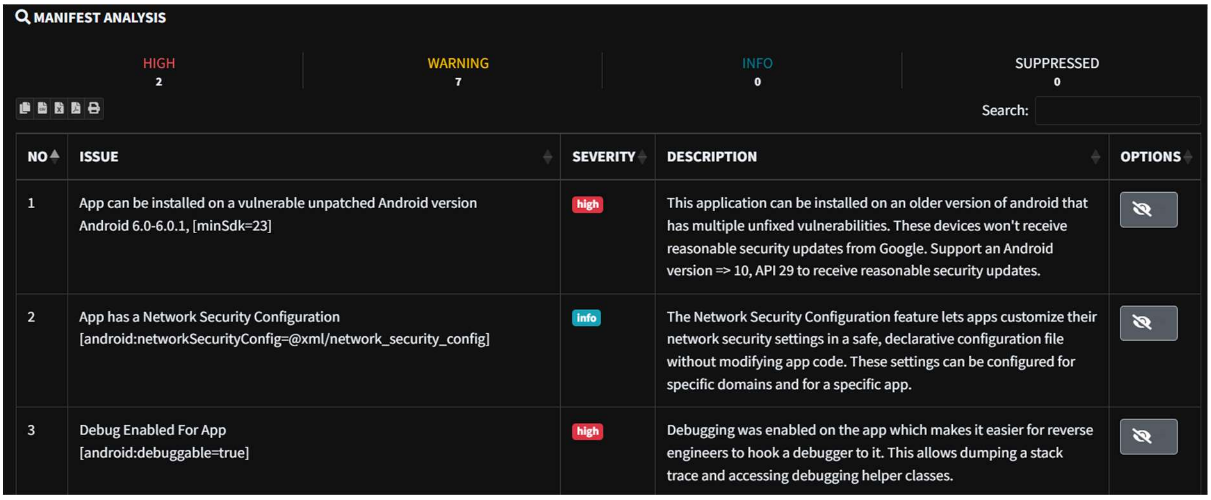
Search:

TITLE	SEVERITY	DESCRIPTION
Application signed with debug certificate	high	Application signed with a debug certificate. Production application must not be shipped with a debug 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.
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.
Signed Application	info	Application is signed with a code signing certificate

Showing 1 to 4 of 4 entries

Manifest analysis

Problem: -



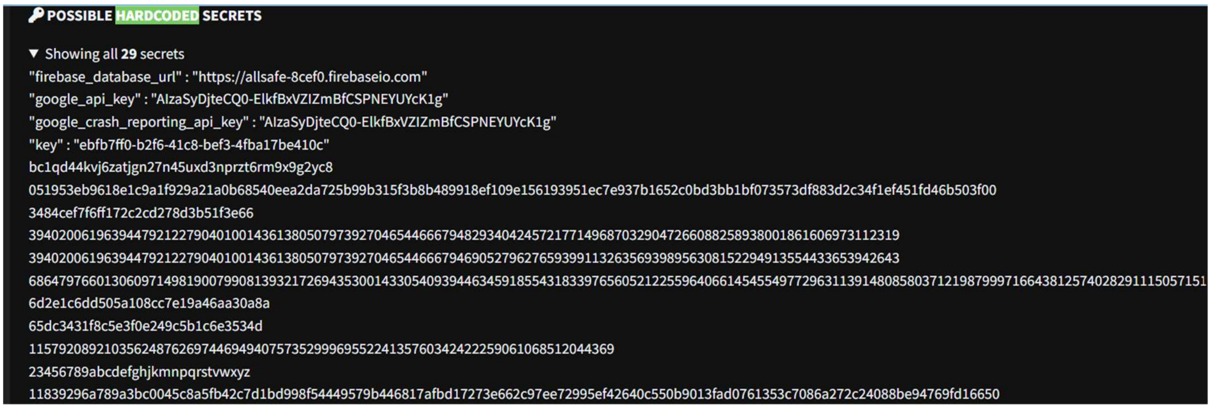
MANIFEST ANALYSIS

HIGH 2 | WARNING 7 | INFO 0 | SUPPRESSED 0

Search:

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.	

Possible hardcoded secrets



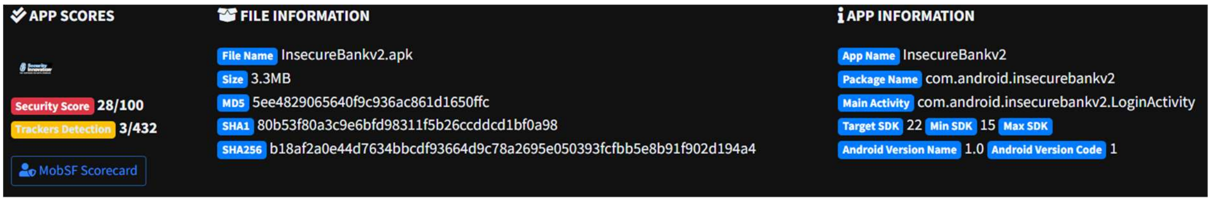
POSSIBLE HARDCODED SECRETS

▼ Showing all **29** secrets

```
"firebase_database_url" : "https://allsafe-8cef0.firebaseio.com"
"google_api_key" : "AIzaSyDjteCQ0-ElkfBxVZIZmBfCSPNEYUYcK1g"
"google_crash_reporting_api_key" : "AIzaSyDjteCQ0-ElkfBxVZIZmBfCSPNEYUYcK1g"
"key" : "ebfb7ff0-b2f6-41c8-bef3-4fba17be410c"
bc1qd44kvj6zatjgn27n45uxd3nprzt6rm9x9g2yc8
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
3484cef7f6ff172c2cd278d3b51f3e66
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
6d2e1c6dd505a108cc7e19a46aa30a8a
65dc3431f8c5e3f0e249c5b1c6e3534d
115792089210356248762697446949407573529996955224135760342422259061068512044369
23456789abcdefghjkmnpqrstvwxyz
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
```

2)Using app InsecureBankV2

File Hash



APP SCORES

Security Score 28/100

Trackers Detection 3/432

MobSF Scorecard

FILE INFORMATION

File Name InsecureBankv2.apk

Size 3.3MB

MD5 5ee4829065640f9c936ac861d1650ffc

SHA1 80b53f80a3c9e6bfd98311f5b26ccddcd1bf0a98

SHA256 b18af2a0e44d7634bbcdf93664d9c78a2695e050393fcfbb5e8b91f902d194a4

APP INFORMATION

App Name InsecureBankv2

Package Name com.android.insecurebankv2

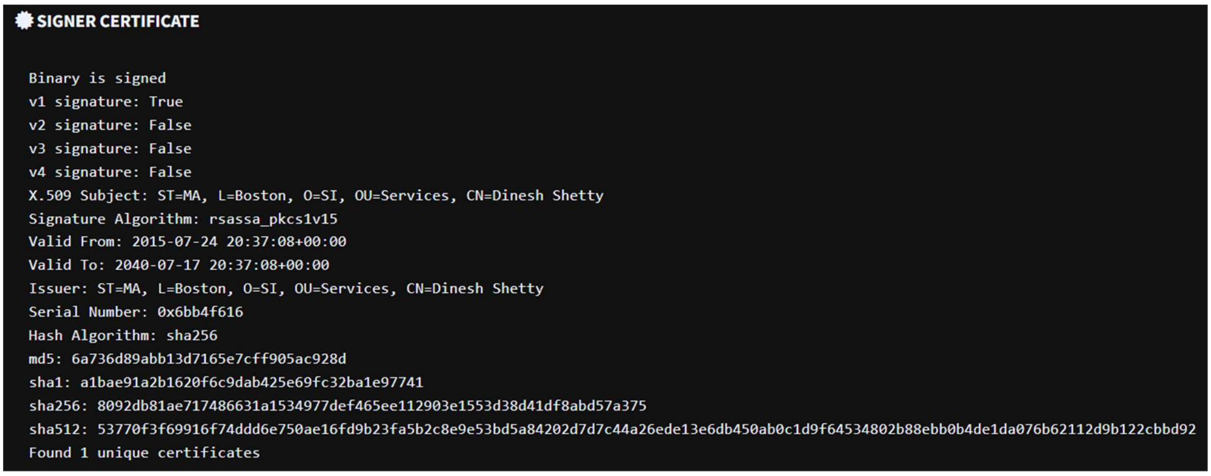
Main Activity com.android.insecurebankv2.LoginActivity

Target SDK 22 Min SDK 15 Max SDK

Android Version Name 1.0 Android Version Code 1

Signer certificate

Problem- V2,V3,V4 signature not available ,not secure

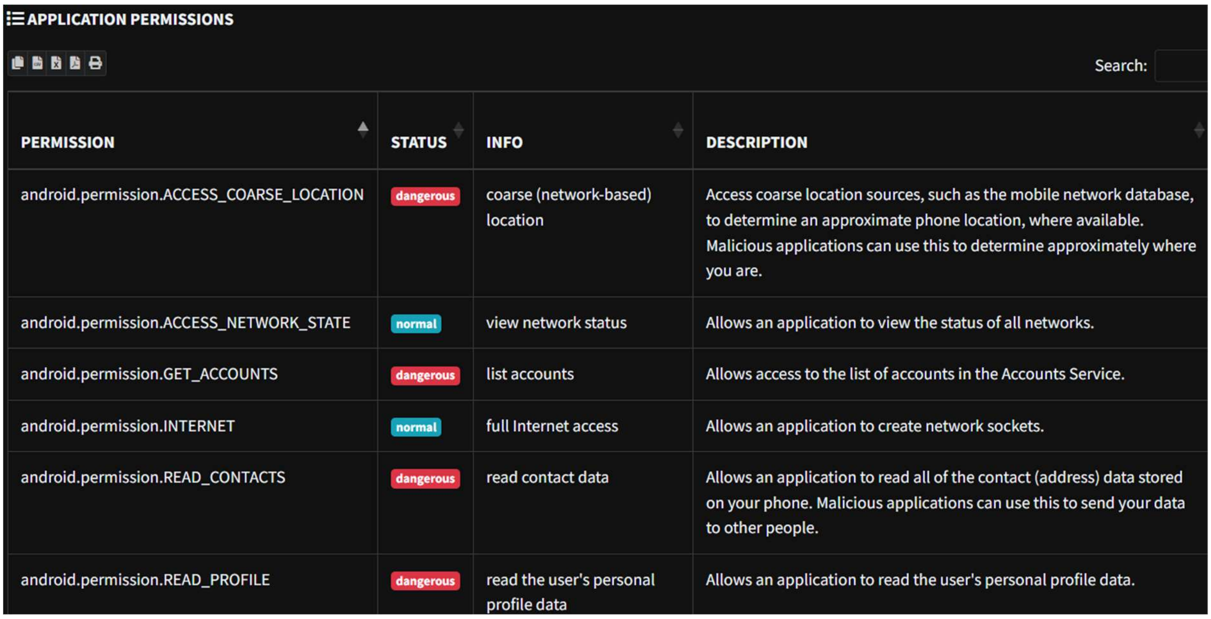


SIGNER CERTIFICATE

```
Binary is signed
v1 signature: True
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: ST=MA, L=Boston, O=SI, OU=Services, CN=Dinesh Shetty
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-07-24 20:37:08+00:00
Valid To: 2040-07-17 20:37:08+00:00
Issuer: ST=MA, L=Boston, O=SI, OU=Services, CN=Dinesh Shetty
Serial Number: 0x6bb4f616
Hash Algorithm: sha256
md5: 6a736d89abb13d7165e7cff905ac928d
sha1: a1bae91a2b1620f6c9dab425e69fc32ba1e97741
sha256: 8092db81ae717486631a1534977def465ee112903e1553d38d41df8abd57a375
sha512: 53770f3f69916f74ddd6e750ae16fd9b23fa5b2c8e9e53bd5a84202d7d7c44a26ede13e6db450ab0c1d9f64534802b88ebb0b4de1da076b62112d9b122cbbd92
Found 1 unique certificates
```

Application permission

Problem – high risk

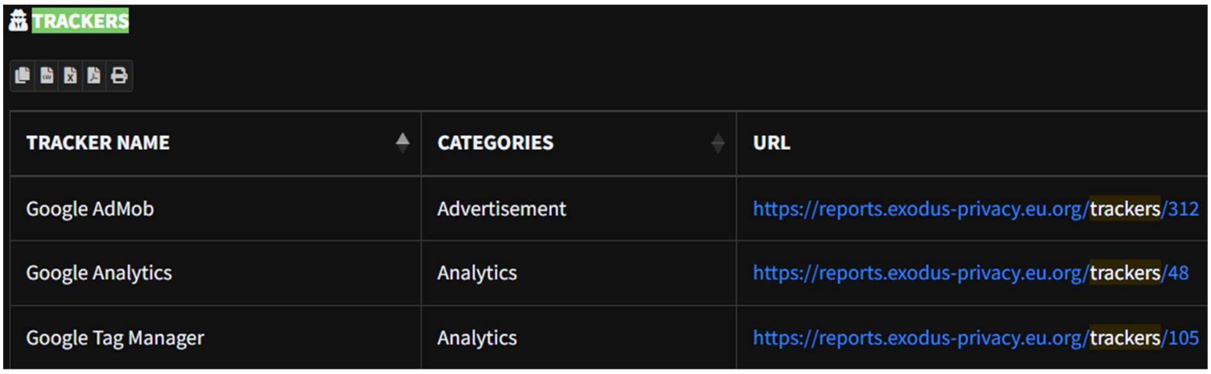


APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION
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.

Trackers Available

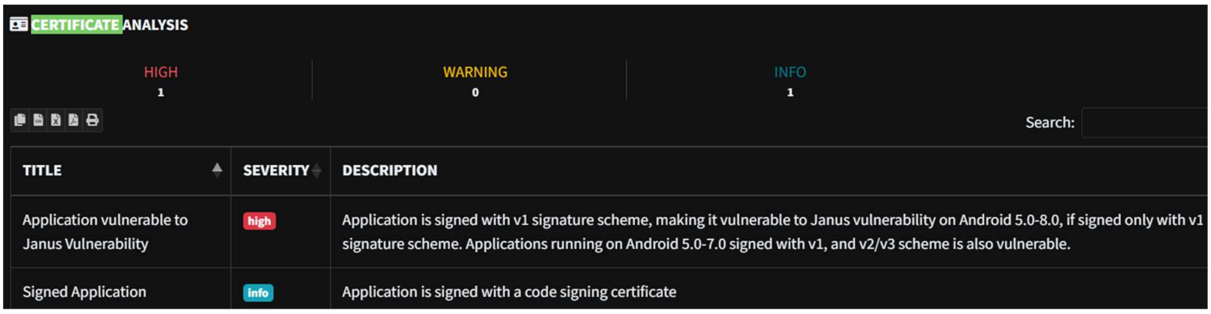


TRACKERS

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

Certificate analysis

Problem-Vulnerability exist



CERTIFICATE ANALYSIS

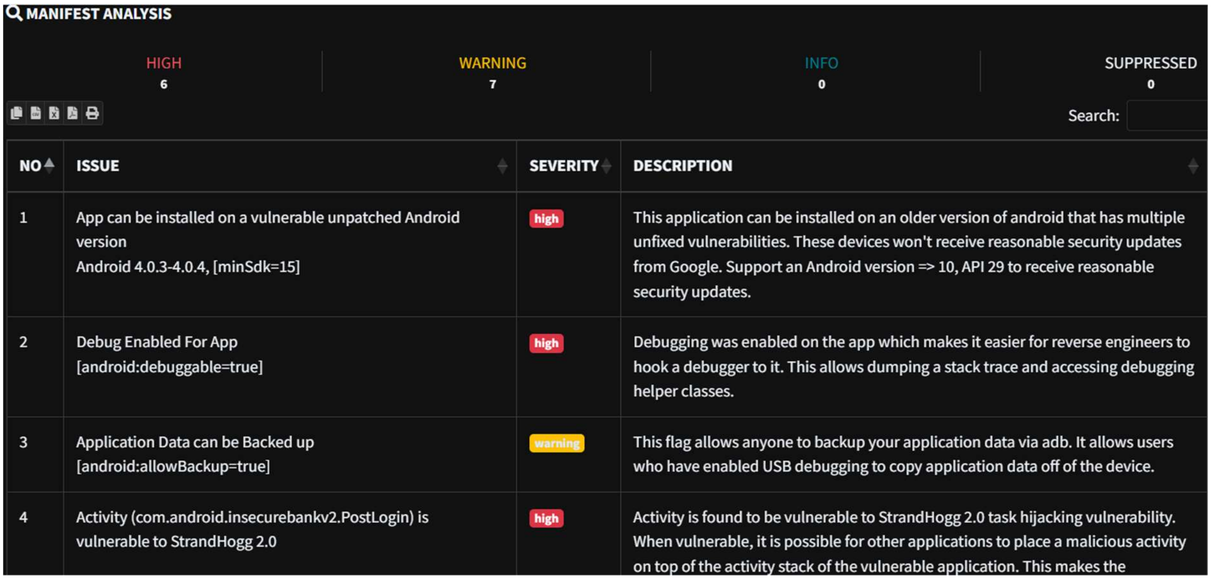
HIGH 1 | WARNING 0 | INFO 1

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

Manifest analysis

Problem: - High Severity



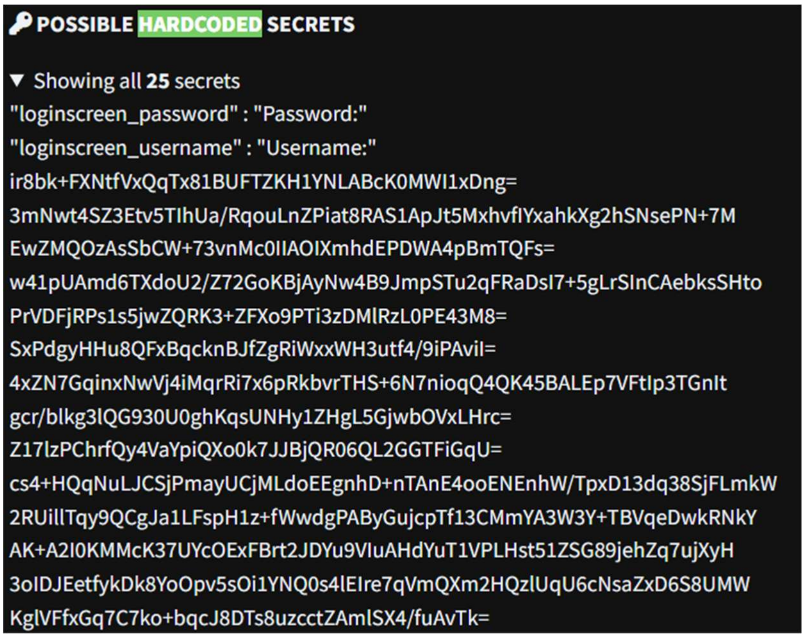
MANIFEST ANALYSIS

HIGH 6 | WARNING 7 | INFO 0 | SUPPRESSED 0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION
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

Possible hardcoded secrets exist



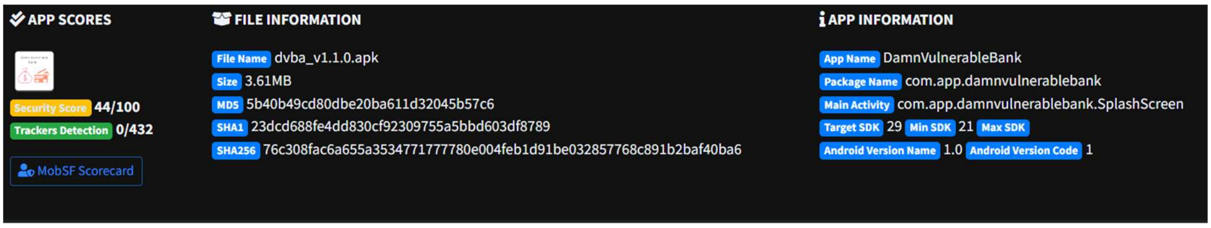
POSSIBLE HARDCODED SECRETS

▼ Showing all **25** secrets

```
"loginscreen_password" : "Password:"
"loginscreen_username" : "Username:"
ir8bk+FXNtfVxQqTx81BUFTZKH1YNLABcK0MWI1xDng=
3mNwt4SZ3Etv5TIhUa/RqouLnZPiat8RAS1ApJt5MxhvflYxahkXg2hSNsePN+7M
EwZMQOzAsSbCW+73vnMc0IIAOIXmhdEPDWA4pBmTQFs=
w41pUAmd6TXdoU2/Z72GoKBjAyNw4B9JmpSTu2qFRaDsI7+5gLrSInCAebksSHto
PrVDFjRPs1s5jwZQRK3+ZFXo9PTi3zDMlRzL0PE43M8=
SxPdgyHHu8QFxBqcknBJfZgRiWxxWH3utf4/9iPAviI=
4xZN7GqinxNwVj4iMqrRi7x6pRkbvrTHS+6N7nioqQ4QK45BALEp7VFtIp3TGnIt
gcr/blkg3lQG930U0ghKqsUNHy1ZHgL5GjwbOVxLHrc=
Z17lzPChrfQy4VaYpiQXo0k7JJBjQR06QL2GGTFiGqU=
cs4+HQqNuLJCSjPmayUCjMLdoEEgnhD+nTAnE4ooENEnhW/TpxD13dq38SjFLmkW
2RUillTqy9QCgJa1LFspH1z+fWwdgPAByGujcpTf13CMmYA3W3Y+TBVqeDwkRNkY
AK+A2I0KMMcK37UYcOExFBrt2JDYu9VIuAHdYuT1VPLHst51ZSG89jehZq7ujXyH
3oIDJEetfykDk8YoOpv5sOi1YNQ0s4lEIre7qVmQXm2HQzlUqU6cNsaZxD6S8UMW
KglVFfxGq7C7ko+bqcJ8DTs8uzcctZAmlSX4/fuAvTk=
```

3) using application DVBA

File Hash



APP SCORES

Security Score 44/100

Trackers Detection 0/432

MobSF Scorecard

FILE INFORMATION

File Name dvba_v1.1.0.apk

Size 3.61MB

MD5 5b40b49cd80dbe20ba611d32045b57c6

SHA1 23dcd688fe4dd830cf92309755a5bbd603df8789

SHA256 76c308fac6a655a3534771777780e004feb1d91be032857768c891b2baf40ba6

APP INFORMATION

App Name DamnVulnerableBank

Package Name com.app.damnvulnerablebank

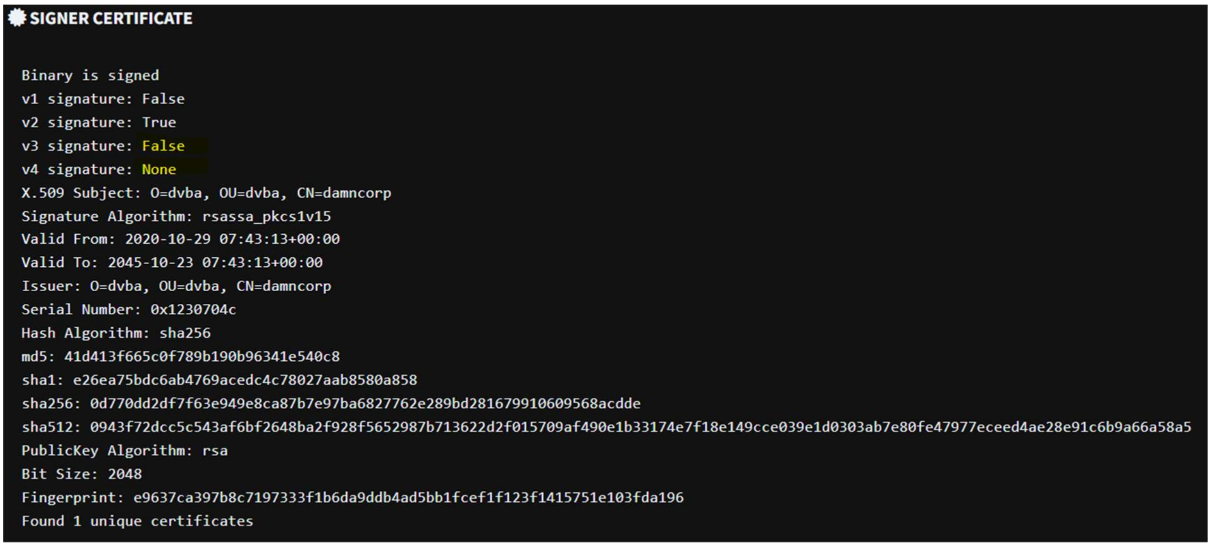
Main Activity com.app.damnvulnerablebank.SplashScreen

Target SDK 29 Min SDK 21 Max SDK

Android Version Name 1.0 Android Version Code 1

Signer certificate note secure

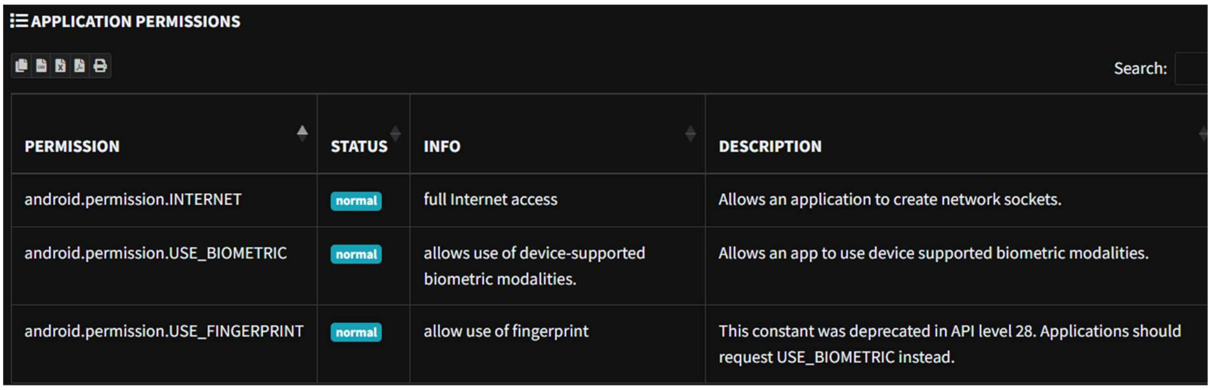
V3 and v4 not secure



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: rsassa_pkcs1v15
Valid From: 2020-10-29 07:43:13+00:00
Valid To: 2045-10-23 07:43:13+00:00
Issuer: O=dvba, OU=dvba, CN=damncorp
Serial Number: 0x1230704c
Hash Algorithm: sha256
md5: 41d413f665c0f789b190b96341e540c8
sha1: e26ea75bdc6ab4769acedc4c78027aab8580a858
sha256: 0d770dd2df7f63e949e8ca87b7e97ba6827762e289bd281679910609568acdde
sha512: 0943f72dcc5c543af6bf2648ba2f928f5652987b713622d2f015709af490e1b33174e7f18e149cce039e1d0303ab7e80fe47977eceed4ae28e91c6b9a66a58a5
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: e9637ca397b8c7197333f1b6da9ddb4ad5bb1fcef1f123f1415751e103fda196
Found 1 unique certificates
```

Application permission

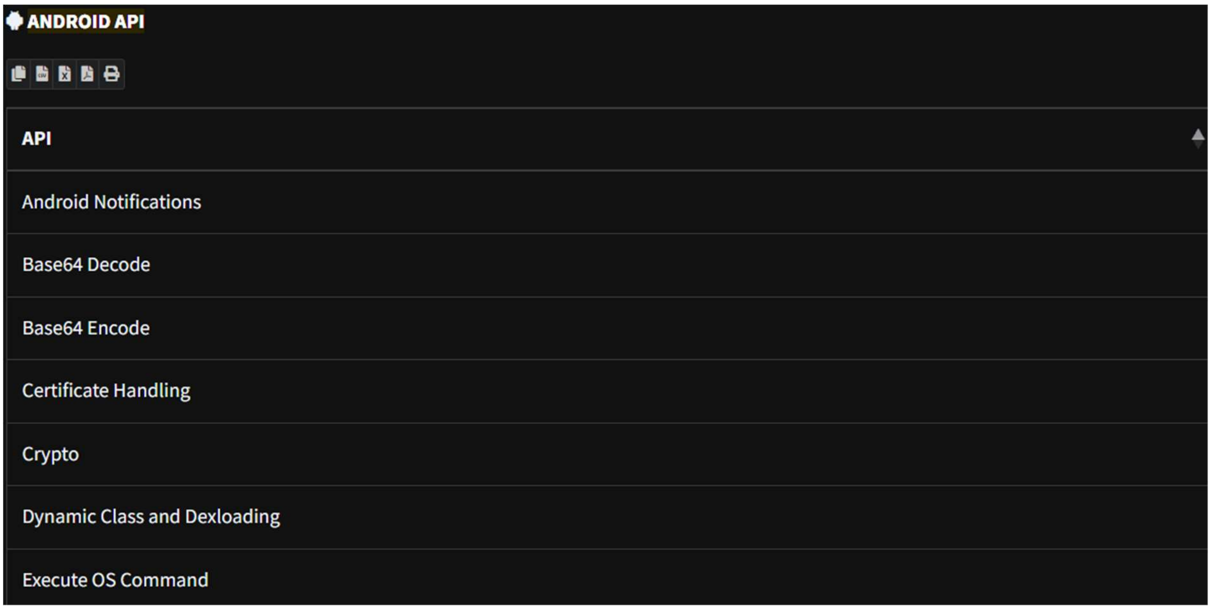


APPLICATION PERMISSIONS

Search:

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

Android API

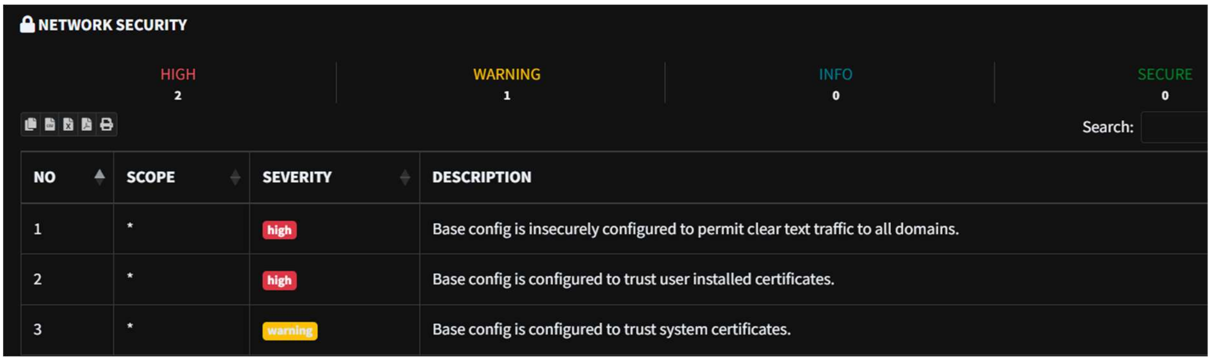


ANDROID API

API
Android Notifications
Base64 Decode
Base64 Encode
Certificate Handling
Crypto
Dynamic Class and Dexloading
Execute OS Command

Network security

Problem: -High risk exist



NETWORK SECURITY

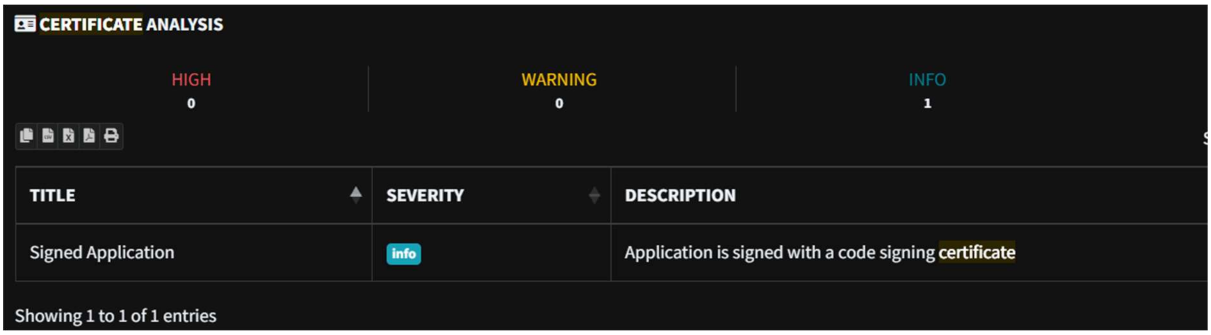
HIGH	WARNING	INFO	SECURE
2	1	0	0

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.

Certificate Analysis

Secure



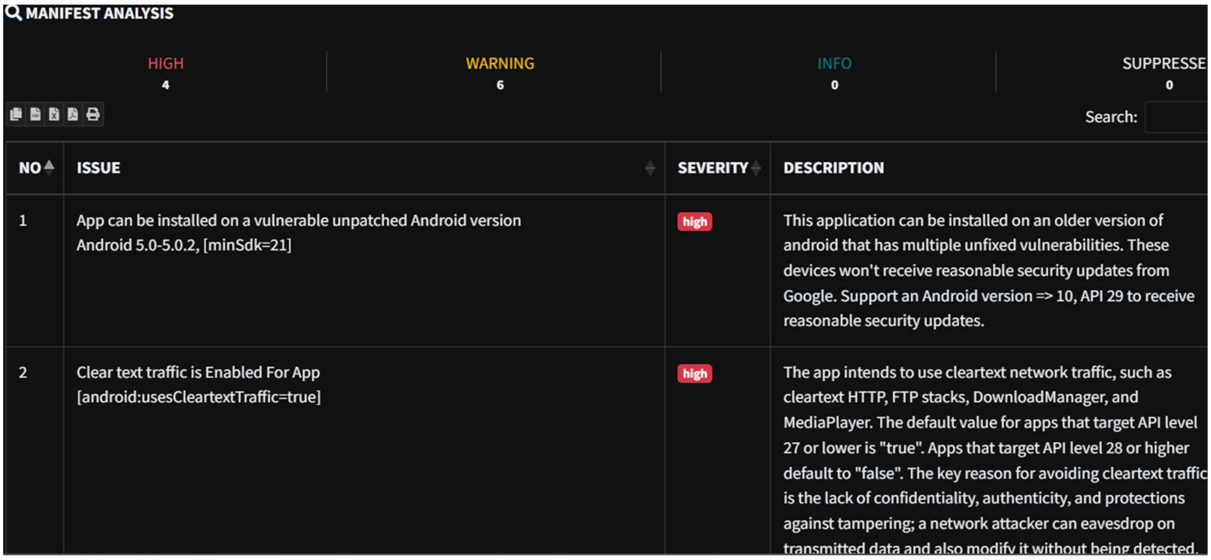
CERTIFICATE ANALYSIS

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

Showing 1 to 1 of 1 entries

Manifest analysis

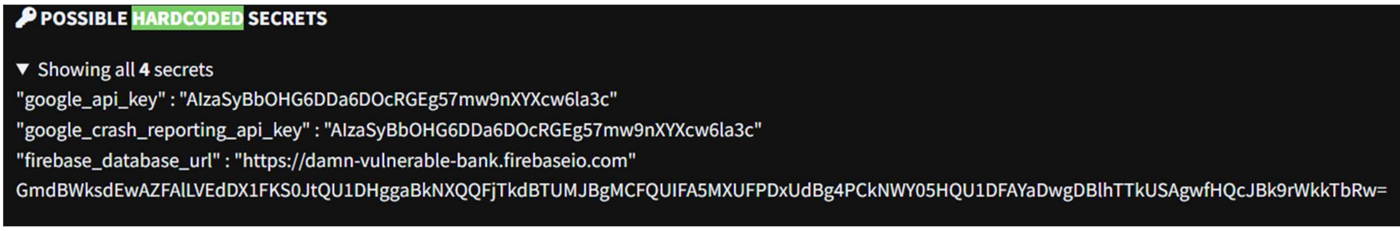
Problem exist- High Risk



MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
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.

Possible Hardcoded secrets Exist

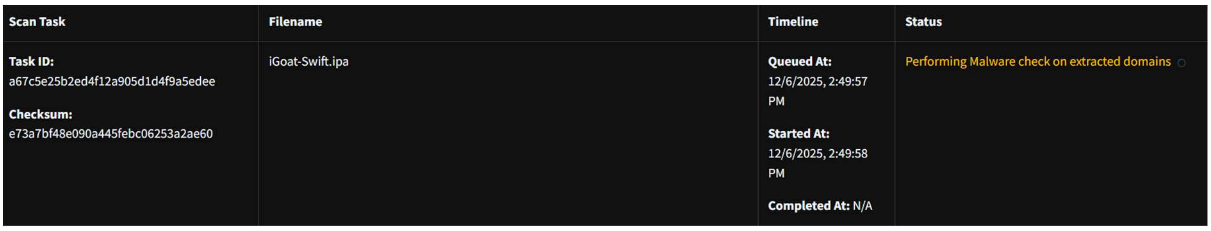


POSSIBLE HARDCODED SECRETS

▼ Showing all **4** secrets

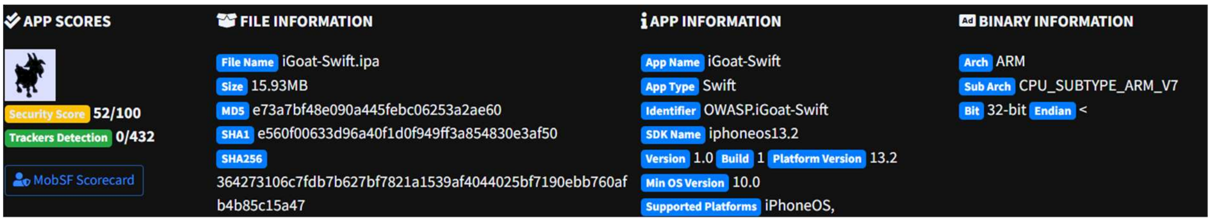
```
"google_api_key" : "AIzaSyBbOHG6DDa6DOcRGEg57mw9nXYXcw6la3c"
"google_crash_reporting_api_key" : "AIzaSyBbOHG6DDa6DOcRGEg57mw9nXYXcw6la3c"
"firebase_database_url" : "https://damn-vulnerable-bank.firebaseio.com"
GmdBWksdEwAZFAlLVEdDX1FKS0JtQU1DHggaBkNXQQFjTkdBTUMJBgMCFQUIFA5MXUFPDxUdBg4PCkNWY05HQU1DFAYaDwgDBlhTTkUSAgwfHQcJBk9rWkkTbRw=
```

4) **using application iGoat igoat.ipa (IOS app)**



Scan Task	Filename	Timeline	Status
Task ID: a67c5e25b2ed4f12a905d1d4f9a5edee **Checksum:** e73a7bf48e090a445febc06253a2ae60	iGoat-Swift.ipa	**Queued At:** 12/6/2025, 2:49:57 PM **Started At:** 12/6/2025, 2:49:58 PM **Completed At:** N/A	Performing Malware check on extracted domains

File Hash info available



APP SCORES

Security Score 52/100

Trackers Detection 0/432

FILE INFORMATION

File Name iGoat-Swift.ipa

Size 15.93MB

MD5 e73a7bf48e090a445febc06253a2ae60

SHA1 e560f00633d96a40f1d0f949ff3a854830e3af50

SHA256 364273106c7fdb7b627bf7821a1539af4044025bf7190ebb760afb4b85c15a47

APP INFORMATION

App Name iGoat-Swift

App Type Swift

Identifier OWASP.iGoat-Swift

SDK Name iphoneos13.2

Version 1.0 Build 1 Platform Version 13.2

Min OS Version 10.0

Supported Platforms iPhoneOS,

BINARY INFORMATION

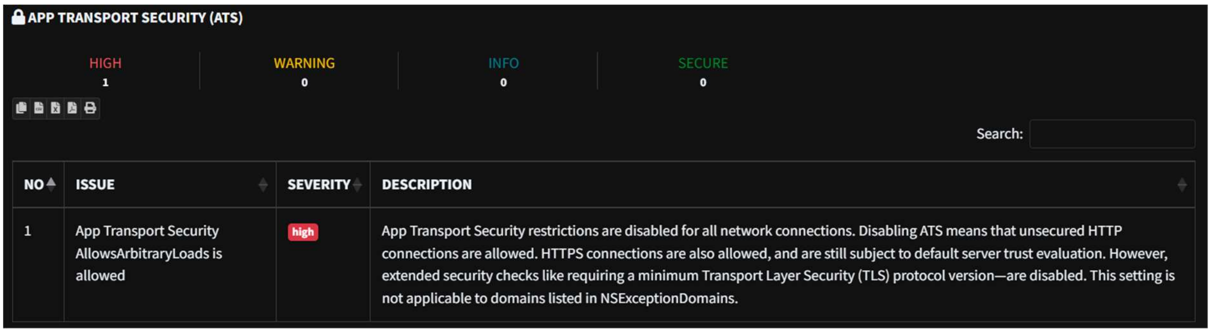
Arch ARM

Sub Arch CPU_SUBTYPE_ARM_V7

Bit 32-bit Endian <

ATS

High Risk exist



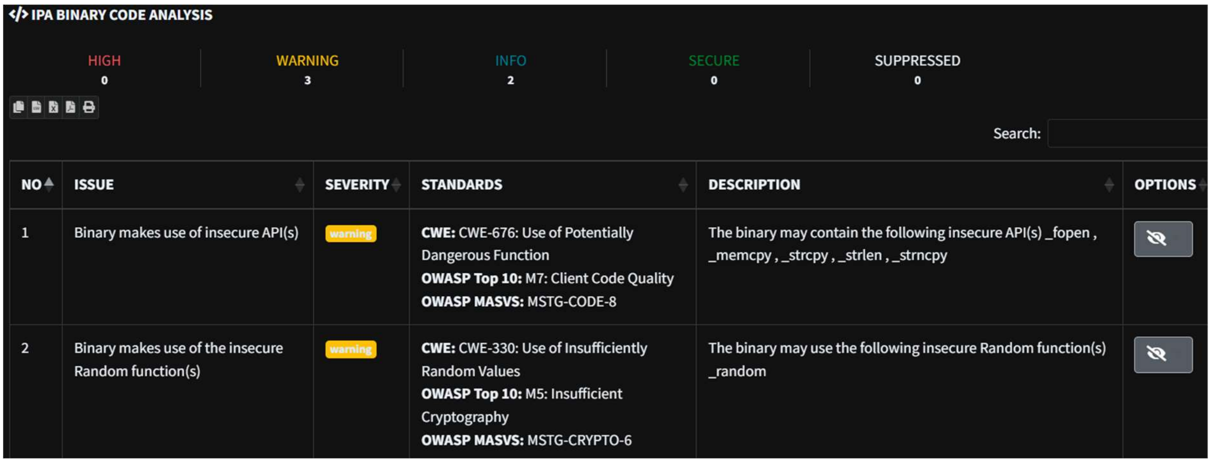
APP TRANSPORT SECURITY (ATS)

HIGH	WARNING	INFO	SECURE
1	0	0	0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App Transport Security AllowsArbitraryLoads is allowed	high	App Transport Security restrictions are disabled for all network connections. Disabling ATS means that unsecured HTTP connections are allowed. HTTPS connections are also allowed, and are still subject to default server trust evaluation. However, extended security checks like requiring a minimum Transport Layer Security (TLS) protocol version—are disabled. This setting is not applicable to domains listed in NSExceptionDomains.

Binary code analysis

Unsafe



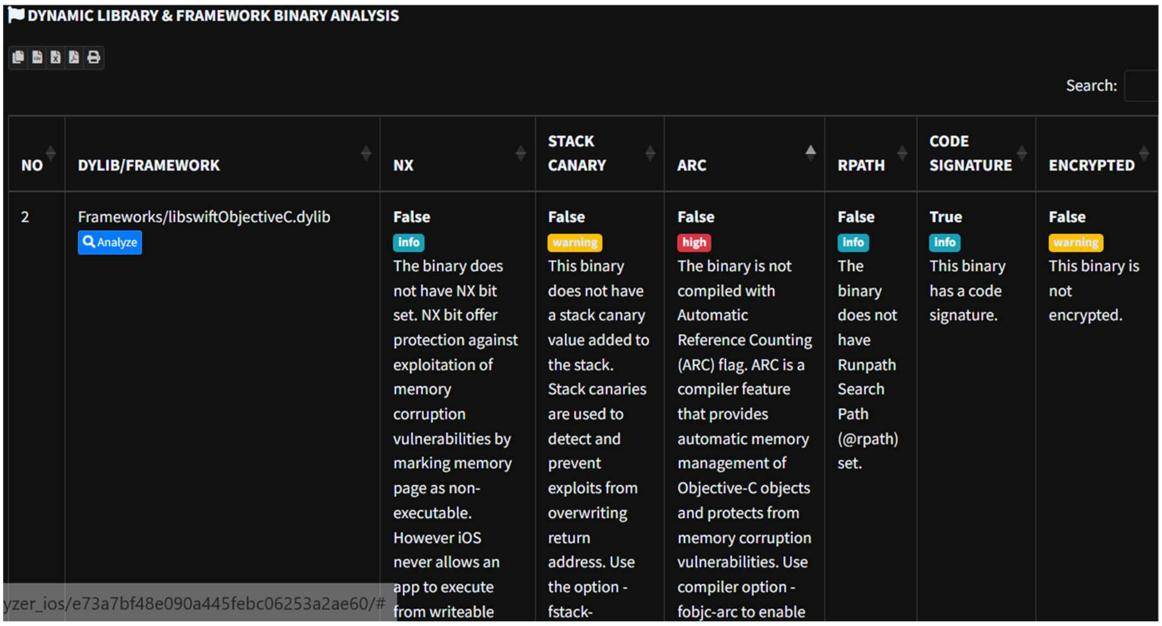
IPA BINARY CODE ANALYSIS

HIGH	WARNING	INFO	SECURE	SUPPRESSED
0	3	2	0	0

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	

Framework analysis

Problem exist high risk

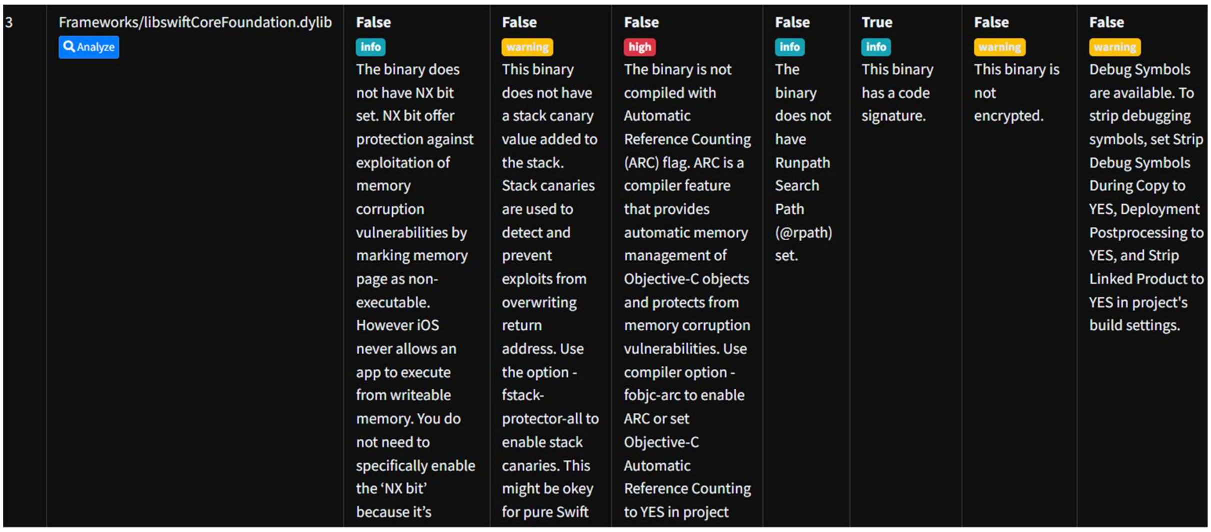


DYNAMIC LIBRARY & FRAMEWORK BINARY ANALYSIS

Search:

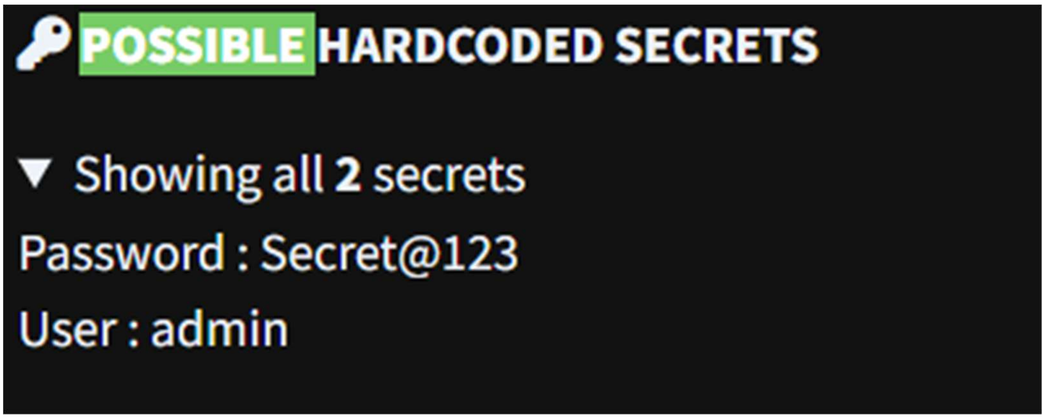
NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED
2	Frameworks/libswiftObjectiveC.dylib Analyze	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable	False warning 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-	False high 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	False info The binary does not have Runpath Search Path (@rpath) set.	True info This binary has a code signature.	False warning This binary is not encrypted.

yzer_ios/e73a7bf48e090a445febc06253a2ae60/#



3	Frameworks/libswiftCoreFoundation.dylib Analyze	False info 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	False warning 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	False high 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	False info The binary does not have Runpath Search Path (@rpath) set.	True info This binary has a code signature.	False warning This binary is not encrypted.	False warning 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



POSSIBLE HARDCODED SECRETS

▼ Showing all 2 secrets

Password : Secret@123

User : admin