

Assignment 6 – Static Analysis (Android & iOS)

1. Static Analysis of Android App

(A.) Allsafe

✓ Information

all basic info about application

The screenshot shows the Allsafe static analysis interface. At the top, there's a navigation bar with links for RECENT SCANS, STATIC ANALYZER, DYNAMIC ANALYZER, API, DONATE, DOCS, ABOUT, and a SEARCH bar. Below the navigation is a section titled 'APP SCORES' with a 'MobSF Scorecard' icon. To the right, under 'FILE INFORMATION', details are provided for 'allsafe.apk': File Name, Size (10.39MB), MD5, SHA1, and SHA256. Further right is the 'APP INFORMATION' section with details like App Name (Allsafe), Package Name (infosecadventures.allsafe), Main Activity (infosecadventures.allsafe.MainActivity), Target SDK (35), and Android Version Name (1.5). Below these sections are four cards: 'EXPORTED ACTIVITIES' (2/4), 'EXPORTED SERVICES' (1/2), 'EXPORTED RECEIVERS' (2/2), and 'EXPORTED PROVIDERS' (1/4). At the bottom left is a 'SCAN OPTIONS' panel with buttons for Rescan, Manage Suppressions, Start Dynamic Analysis, and Scan Logs. On the right is a 'DECOMPRESSED CODE' panel with links to view AndroidManifest.xml, source code, small code, and download Java Code, Small Code, and APK.

✓ SIGNER CERTIFICATE

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

This screenshot shows the 'SIGNER CERTIFICATE' section of the Allsafe interface. It displays detailed information about the certificate, including its signature type (v1, v2, v3, v4), subject (CN=Android Debug, O=Android, C=US), signature algorithm (rsassa_pkcs1v15), and various hash algorithms (sha1, sha256, sha384, sha512). The certificate was issued on 2022-06-28 and valid until 2052-06-20. The public key algorithm is RSA with a bit size of 2048, and the fingerprint is d4600cd715a831571dc15583b841cbc51bd51e2fc7b0191b76b7006a5303250d. A note at the bottom states '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 File
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 File
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.	Show File
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.	Show File
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		FILES
API		Show File
Local File I/O Operations		Show File
Crypto		Show File
Message Digest		Show File
Loading Native Code (Shared Library)		Show File
TCP Socket		Show File
Starting Activity		Show File
Inter Process Communication		Show File
Starting Service		Show File
Base64 Decode		Show File
Dynamic Class and Dexloading		Show File
Get Installed Applications		Show File
WebView GET Request		Show File
Get System Service		Show File
Android Notifications		Show File
Sending Broadcast		Show File
Set or Read Clipboard data		Show File
Java Reflection		Show File
Execute OS Command		Show File
Content Provider		Show File

✓ NETWORK SECURITY

issue:- insecurely configured

NETWORK SECURITY			
HIGH	WARNING	INFO	SECURE
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

MANIFEST ANALYSIS			
HIGH 2	WARNING 7	INFO 0	SUPPRESSED 0
NO	ISSUE	SEVERITY	DESCRIPTION
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		
TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firbaseremoteconfig.googleapis.com/v1/projects/983632160629/namespaces.firebaseio.fetch?key=AlzaSyDjeCQ0-ElkfbVzIZmBfCSPNEYUyK1g. 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

✓ POSSIBLE HARDCODED SECRETS

issue:- secret keys and api keys leaked

```

POSSIBLE HARDCODED SECRETS
▼ Showing all 29 secrets
"google_api_key": "AIzaSy0teCQD-EIkBrVZlZmBICSPNEYUck1g",
"key": "1ibf7ff0-b2f4-1c8-be73-fab17be410c",
"firebase_database_url": "https://callsafe-8cf0.firebaseio.com",
"google_crash_reporting_api_key": "AIzaSy0teCQD-EIkBrVZlZmBICSPNEYUck1g",
c6859e00b7d7404e0d953ec6b62335b442c648139053fb521f82a8af0064d3dbaa14b5e77fe75928fe1dc127a2fa8de3348b3c1856a429bf97e7e31c2e5bd66
1835c58e866aa69c48ef633243277f28af5d4b4
aa87ca22beeb0537be1c17ef20ad746e1d3b62ba09e162bce3357fb315ececcb6406837bf515
258EFA5-E914-47D4-95CA-CSAB0D65B11
bc1q444vqyfatgn27n+5uxw3npri0fm9xg3yc8
0af58729667eace3883a992a2b0c6e29
11839296789a3bc045c8a5fb42c7d1bd598f54449579b44681tfd17273e662c97ee172995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
5ac635d0aa93e793e73e6bd557f986bb6c51d06b0c53b0f3bce3c2726d4b
384cef7ff6f172c2d7835151e66
6b17d1f2a12c4247f8bceee933444f977037d812deb33a0f4a13945d898c296
6d2e1cd455a5108c7e19a46a3a0a8a
2345678abcfedghkmnpqrstuvwxyz
051953e9618e1e91f29a21a0b685400e2d075959b315fb84b9918ef109e15613951eect937b1652c0bd3bb1bf73573dff883d2c341e451f1d46b50300
68647976601306097149819007990813932172694353001433054093944643a591855431833975605212255964066145454977296311391480858037121987999716643812574028291115057151
11579208921035624876269744694940757535300614341529031419553363130886709785391
6543d34318c530e249c5b1ce3534d
d510890806278e664f119581eb7cf
68647976601306097149819007990813932172694353001433054093944634591855431833976553942450577463332117197532963996371363321113864768612440380340372808892707005449
394020061963944792122790401001436138050797392704654466794829340424572177149687032904726608259338001861606973112319
3617644963262c6f5d9e98bf9292d429bf41dbd289a147c9da3113b5f0b8c0a60b1ce1d7e819d7a431d7c90ea0e5f
21232f297a57a43894a0e4a8013

```

(B.) InsecureBankV2

✓ Information

all basic info about application

APP SCORES

Security score: 28/100
Trackers detected: 3/432
MobSF Scorecard

FILE INFORMATION

File Name: InsecureBankV2.apk
Size: 3.3MB
MD5: 5e64d2905640fb9c936ac861d1e50fc
SHA1: 4b053fb03a3c9ebfd98311fb5b2ccddcd1bf0a88
SHA256: b18af2a0a44d7634b4bcdff33664d9c78a2095e050393cfbb5e8091f902d194a8

APP INFORMATION

App Name: InsecureBankV2
Package Name: com.android.insecurebankv2
Main Activity: com.android.insecurebankv2.LoginActivity
Target SDK: 22 Min SDK: 15 Max SDK: 1
Android Version Range: 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: ST=MA, L=Boston, O=SI, OU=Services, CN=Dinesh Shetty
Signature Algorithm: RSA-SHA1
Valid From: 2015-07-24 20:31:08+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: 0xb0d4f616
Hash Algorithm: sha256
nd5: 0a736068113d7105e7cff908ac926d
sha1: a115349770425e6097c32b41e77741
sha256: 8092d091a27480e31a15349770425e6097c32b41e77741
sha512: 5377073f5f9916f774d666e730ae10fd8b23fa92c8e0e53bd5a84292d707c44a2ede13e6db45348002b88eb0b4de1da070b62112d9b122cb92

Found 1 unique certificates

✓ APPLICATION PERMISSIONS

issue: unwanted permission as shown in ss

APPLICATION PERMISSIONS					Search: <input type="text"/>
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			Search: <input type="text"/>
HIGH	WARNING	INFO	
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

Q. MANIFEST ANALYSIS			
	HIGH 6	WARNING 7	INFO 0
NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 4.0-3.4.0, [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+73vnMc0lIA0lxmhEDPdWA4pBmTQFs=
AK+A210KMmcK37UyC0ExBrt2JDYu9ViuAHdvt1VPLHst51ZSG89jehZq7ujxjYH
2RUlllTqy9QCgJa1LFspH1z+fIWwdgPAByGujcptf13CMmY3W3Y+TBVqeDwkRNkY
w41puAmd6Txd0u2/Z72gokBjAyNw4B9JmpStu2qFRadsl7+5gLrSlcAebksSHt0
Fych2TPIScbLjxRidoDvUow7d3sVUDiaLAvtmpgWr8g7e+3+ib/JMLjt3rf841gO
VECoKG0ld10uMkpilFK462ikClkVyy7m55v4INe3KRY=
3oIDJEtfykDk8YoOpv5s01YNQ0s4lElr7qVmQxm2HqzlUql6cNsazxD658UMW
M/9MnPtadNnPsJGLBqvtaLid0g4JyMoqf5ncPhI=
KglVfGg7C7ko+bqcJB8DTs8uzcctZAmSX4/fuAvTk=
gcr/blkg3lQG930U0ghKqsUNHy1ZHg5JgwboVxLHrc=
6NX7jQU62u42sQ68cog9+pwW2l0P1J/qqDEEENU4ZU=
eRIYZ7vvE2B0WWejblqyBziYzuBt9JW024X3YOHX2VY=
Z17LzChrfoQ4vAypQx0ok7JBjQR06QL2GGTFigQu=
MU3VGnFcuvu612xEKn6ZfJFowurNeeRHlUpI0GcgsFQ=
cs4+H0qNulJCSjpmayUCjMLdoEEgnhd+nTAnE4ooENEnhW/TpxD13dq38SjFLmkW
qfDkyRzITZGguvBzojuWMEqfl8Qqw5CcMB2eo7wr2iH9X2v+qIFOYnd9v9ffS1x0
4xZN7GqinxNWVj4lMqr7x6pRkbvrTHs+6N7niqQ4QK45BAleP7Vftlp3TGnit
3mNwt4523Ev5TlhUa/RqouLnZPiat8RA51ApJt5Mxhvf1YxahhXg2hSNsePN+7M
PrVDfRP1s5jwZQRK3+ZFx9PT1zDMlRzL0PE43M8=
SxPdgjHHu8QfwBqcknBjfZgRiWxWH3utf4/9IPAvil=
ir8bk+FXTnfVxQqTx81BUFTZKH1YNLAbckOMW11xDng=
Y6D/Yzc0CnVSZ/savV5VKYCoaQyT30gvMdLessm7RE=
FaKwm3zfk+Dhq4JqMMBs2A+ODqwwgRuoVlqzQMyOaB4=
```

(C.) DVBA

✓ Information

all basic info about application

APP SCORES

FILE INFORMATION

APP INFORMATION

EXPORTED ACTIVITIES: 5 / 19

EXPORTED SERVICES: 0 / 1

EXPORTED RECEIVERS: 0 / 0

EXPORTED PROVIDERS: 0 / 1

SCAN OPTIONS

DECOMPILATED 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: False
v5 signature: False
X.509 Subject: CN=dvba, OU=dvba, O=damncorp
Signature Algorithm: rsaSSP_pcks1v15
Valid From: 2020-10-29 07:43:13+00:00
Valid To: 2045-10-23 07:43:13+00:00
Issuer: CN=dvba, OU=dvba, O=damncorp
Serial Number: 10000000000000000000000000000000
Hash Algorithm: sha256
MD5: A1d413f0d5c2f780b19eb00341e540c8
sha1: e26ea7bdca8a47909a0cedc4c78027aab8580a858
sha256: 0d770dd2df7f63e949c8a87b7e97b86827762e280bd2816799106099568acd4
sha512: 0043f72dc5c543af8bf2648ba2f928f5852987b713622d2f015709af490e1b33174e7f18e149cce039e1d0303ab7e80fe47977eced4ae28e91c6b9a66a58a5
Publickey Algorithm: rsa
Bit Size: 2048
Fingerprint: e96837ca297b8c7197333f1b6da9db4ad5bb1fce1f123f1415751e103fd196
Found 1 unique certificates

```

✓ APPLICATION PERMISSIONS

all ok

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

✓ ANDROID API

ANDROID API

API	FILES
Android Notifications	Show File
Base64 Decode	Show File
Base64 Encode	Show File
Certificate Handling	Show File
Crypto	Show File
Dynamic Class and Dexloading	Show File
Execute OS Command	Show File
Get Installed Applications	Show File
Get System Service	Show File
GPS Location	Show File
Showing 1 to 10 of 20 entries	
	Previous Next

✓ NETWORK SECURITY

issue:- insecurely configured

NETWORK SECURITY

HIGH 2	WARNING 1	INFO 0	SECURE 0
			Search: <input type="text"/>
1	High		
2	High		
3	Warning		
Showing 1 to 3 of 3 entries			
			Previous Next

✓ CERTIFICATE ANALYSIS

ok

CERTIFICATE ANALYSIS

HIGH 0	WARNING 0	INFO 1
		Search: <input type="text"/>
Signed Application	Info	Application is signed with a code signing certificate
Showing 1 to 1 of 1 entries		
		Previous Next

✓ MANIFEST ANALYSIS

issue:- multiple issues as shown in ss

Q. MANIFEST ANALYSIS		HIGH 4	WARNING 6	INFO 0	SUPPRESSED 0
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.	Edit Delete	
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	High	The app intends to use cleartext network traffic, such as cleartextHTTP, FTP, Slack, 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.	Edit Delete	
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.	Edit Delete	
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.	Edit Delete	
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 URL, 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.	Edit Delete	
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 URL, 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.	Edit Delete	
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.	Edit Delete	
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.	Edit Delete	
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.	Edit Delete	
10	Activity [android.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.	Edit Delete	

✓ 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	Edit Delete
Firebase Remote Config disabled	Severe	Firebase Remote Config is disabled for https://firebase.remoteconfig.googleapis.com/v1/projects/932398433474/namespaces.firebaseio.fetch?key=AlzaSyBbOHG6DDa6DOcRGEg57mw9nXYXcw6la3c . This is indicated by the response: {state: 'NO_TEMPLATE'}	Edit Delete
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": "AlzaSyBbOHG6DDa6DOcRGEg57mw9nXYXcw6la3c"	
"firebase_database_url": " https://damn-vulnerable-bank.firebaseio.com "	
"google_crash_reporting_api_key": "AlzaSyBbOHG6DDa6DOcRGEg57mw9nXYXcw6la3c"	
GmdBWksdEwAZFAILVEdDX1FKS0JtQU1DHggaBkNXQQFjTkdbTUMJBgMCFQUIFA5MXUFPDxUdBg4PCkNWY05HQU1DFAYaDwgDBlhTTkUSAgwfHQcJBk9rWkkTbRw=	

2. Static Analysis of iOS App

(A.) iGoat

✓ Information

all basic info about application

The screenshot shows the Mobsf interface for analyzing the iGoat-Swift.ipa file. It includes sections for App Scores, File Information, App Information, Binary Information, Scan Options, and Decompiled Assets.

✓ ATS

issue: App Transport Security AllowsArbitraryLoads is allowed

The screenshot shows the App Transport Security (ATS) analysis results. There is one HIGH severity issue: "App Transport Security AllowsArbitraryLoads is allowed". The description states: "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."

✓ APPLICATION PERMISSIONS

ok

The screenshot shows the Application Permissions analysis results. There is one permission entry: NSFaceIDUsageDescription, which is normal and grants access to authenticate with Face ID. The reason in the manifest is "iGoat would like to use FaceID to authenticate you."

✓ 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	0	WARNING	3	INFO	2
SECURE	0	SUPPRESSED	0		
Search: <input type="text"/>					
NO	ISSUE	SEVERITY	STANDARDS	DESCRIPTION	
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) _open, _memcpy, _strcpy, _strlens, _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

Previous Next First Last

✓ FRAMEWORK BINARY ANALYSIS

issues:- many issue as shown in ss

RECENT SCANS STATIC ANALYZER DYNAMIC ANALYZER API DONATE DOCS ABOUT Search										
DYNAMIC LIBRARY & FRAMEWORK BINARY ANALYSIS										
NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED		
1	Frameworks/libswiftFoundation.dylib	False	True	True	False	True	False	False	False	False
2	Frameworks/libswiftObjectiveC.dylib	False	False	False	False	True	False	False	False	False
3	Frameworks/libswiftCoreFoundation.dylib	False	False	False	False	True	False	False	False	False
4	Frameworks/libswiftCoreImage.dylib	False	False	False	False	True	False	False	False	False

✓ POSSIBLE HARDCODED SECRETS

issue:- user password leaked

POSSIBLE HARDCODED SECRETS	
▼ Showing all 2 secrets	
User : admin	
Password : Secret@123	

