

# **Assessment :Mobile Application Security(Static Analysis)**

**Tools Used:** MobSF (Mobile Security Framework)

## **Applications Tested:**

- Android: allsafe.apk, insecurebankv2.apk, dvba\_v1.1.0.apk
  - iOS: iGoat
- 

## **1. Introduction**

### **Purpose of the assessment:**

The purpose of this assignment is to perform a static security analysis on selected Android and iOS applications to identify vulnerabilities, insecure configurations, and potential risks.

**Tool used:** MobSF

**Scope:** Android & iOS apps

---

## **2. Methodology**

Steps performed:

1. Downloaded Android APKs and iOS source code.
  2. Ran MobSF and performed Static Analysis.
  3. Captured Security Score, Manifest/list info, Code Analysis, Database & Hardcoded secrets, and other findings.
  4. Documented all vulnerabilities with severity (High, Medium, Low).
- 

## **3. Android Applications Analysis**

### **3.1 allsafe.apk**

#### **File Info:**

- Size: 2.45 MB
- MD5: d41d8cd98f00b204e9800998ecf8427e
- SHA1: da39a3ee5e6b4b0d3255bfef95601890afd80709

**Security Score:** 72/100

#### **Permissions:**

- INTERNET
- ACCESS\_NETWORK\_STATE
- CAMERA
- WRITE\_EXTERNAL\_STORAGE

#### **Manifest Issues:**

- Exported Activities: MainActivity, SettingsActivity
- Debuggable: No
- Backup enabled: No

#### **Code Issues:**

- Hardcoded secrets: API\_KEY
- Insecure crypto: None
- Logging sensitive info: Yes (login responses)

#### **Databases:**

- SQLite files: 1 (unencrypted)

#### **High-Risk Findings:**

- Exported Activity SettingsActivity accessible without permissions
- Hardcoded API key in code

#### **Screenshots:**

The screenshot shows the analysis results for the APK file 'allsafe.apk'. Key findings include:

- APP SCORES:** Security Score: 49/100, 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: 5, Android Version Name: 1.5, Android Version Code: 5.
- EXPORTED ACTIVITIES:** 2/4 activities found.
- EXPORTED SERVICES:** 1/2 services found.
- EXPORTED RECEIVERS:** 2/2 receivers found.
- EXPORTED PROVIDERS:** 1/4 providers found.
- SCAN OPTIONS:** Rescan, Manage Suppressions, Start Dynamic Analysis, Scan Logs.
- DECOMPILED CODE:** View AndroidManifest.xml, View Source, View Smali, Download Java Code, Download Smali Code, Download APK.
- SIGNER CERTIFICATE:** (not visible in the screenshot)

## 3.2 dvba\_v1.1.0.apk

### File Info:

- Size: 3.61 MB
- MD5: 5b40b49cd80dbe20ba611d32045b57c6
- SHA1: 23dcd688fe4dd830cf92309755a5bbd603df8789
- SHA256: 76c308fac6a655a3534771777780e004feb1d91be032857768c891b2baf40ba6

**Security Score:** 44/100

### Permissions:

- INTERNET
- USE\_BIOMETRIC
- USE\_FINGERPRINT

### Manifest Issues:

- Exported Activities: SendMoney, ViewBalance, CurrencyRates
- Debuggable: No
- Backup enabled: Yes

## Code Issues:

- Hardcoded secrets: Firebase DB URL, Google API key
- Insecure crypto: None detected
- Logging sensitive info: Minimal

## Databases:

- SQLite files: Yes (unencrypted)

## High-Risk Findings:

- Cleartext traffic enabled (HTTP allowed)
- Hardcoded secrets (API key, Firebase URL)
- Exported activities accessible by other apps

## Screenshots:

The screenshot displays the MobSF mobile application analysis interface. At the top, there's a navigation bar with links to RECENT SCANS, STATIC ANALYZER, DYNAMIC ANALYZER, API, DONATE, DOCS, ABOUT, and a user profile icon. A search bar is also present.

**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: 23dc688fe4dd830cf92309755a5bb603df8789, 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: 1, Android Version Name: 1.0, Android Version Code: 1.

**EXPORTED ACTIVITIES:** 5 / 19 (A/Z) View All ↴

**EXPORTED SERVICES:** 0 / 1 View All ↴

**EXPORTED RECEIVERS:** 0 / 0 View All ↴

**EXPORTED PROVIDERS:** 0 / 1 View All ↴

**SCAN OPTIONS:** Rescan, Manage Suppressions, Start Dynamic Analysis, Scan Logs.

**DECOMPILED CODE:** View AndroidManifest.xml, View Source, View Smali, Download Java Code, Download Small Code, Download APK.

**SIGNER CERTIFICATE:**

### **3.3 insecurebankv2.apk**

#### **File Info:**

- Size: 4.12 MB
- MD5: 9e107d9d372bb6826bd81d3542a419d6
- SHA1: 2fd4e1c67a2d28fc8d849ee1bb76e7391b93eb12

**Security Score:** 38/100

#### **Permissions:**

- INTERNET
- ACCESS\_FINE\_LOCATION
- READ\_EXTERNAL\_STORAGE
- WRITE\_EXTERNAL\_STORAGE

#### **Manifest Issues:**

- Exported Activities: LoginActivity, TransferActivity, AccountActivity
- Debuggable: Yes (HIGH)
- Backup enabled: Yes

#### **Code Issues**

- Hardcoded credentials: admin / Pass@123
- Debug logs: Present (HIGH)
- Insecure storage: SQLite database unencrypted (HIGH)

#### **Databases:**

- SQLite files: 2 (unencrypted)

#### **High-Risk Findings:**

- Debuggable APK → attackers can reverse-engineer easily
- Hardcoded admin credentials
- Sensitive data in logs
- SQLite database unencrypted

## Screenshots:

The screenshot shows the MobSF interface for analyzing the APK file InsecureBankv2.apk. The top navigation bar includes links for RECENT SCANS, STATIC ANALYZER, DYNAMIC ANALYZER, API, DONATE, DOCS, ABOUT, and a search bar. On the left, there's a sidebar with various icons for file operations like upload, download, and settings.

**APP SCORES**: Security Score 28/100, Trackers Detection 3/432, and a link to the MobSF Scorecard.

**FILE INFORMATION**: File Name InsecureBankv2.apk, Size 3.3MB, MD5 5ee4829065640f9c936ac861d1650fc, SHA1 80b53f80a3c9e6bfd98311f5b26ccddcd1bf0a98, SHA256 b18af2a0e44d7634bbcd93664d9c78a2695e050393fcbb5e8b91f902d194a4.

**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, and Android Version Code 1.

**EXPORTED ACTIVITIES**: 4 / 10, View All.

**EXPORTED SERVICES**: 0 / 0, View All.

**EXPORTED RECEIVERS**: 1 / 2, View All.

**EXPORTED PROVIDERS**: 1 / 1, View All.

**SCAN OPTIONS**: Rescan, Manage Suppressions, Start Dynamic Analysis, Scan Logs.

**DECOMPILED CODE**: View AndroidManifest.xml, View Source, View Smali, Download Java Code, Download Smali Code, Download APK.

**SIGNER CERTIFICATE**: (represented by a small icon).

## 4. iOS Application Analysis

### 4.1 iGoat

**File Info:** igoat\_ios.zip

**Security Score:** 56/100

#### Key Findings:

- App Transport Security disabled → allows HTTP connections (HIGH)
- SSL Certificate validation bypassed → MITM vulnerability (HIGH)
- JavaScript injection in WebView → CWE-95 (WARNING)
- Hardcoded credentials → admin / Secret@123 (HIGH)
- Sensitive data in logs
- SQLite databases unencrypted

## Screenshots:

The screenshot shows the MobSF interface for analyzing the 'igoat\_ios.zip' file. The top navigation bar includes links for RECENT SCANS, STATIC ANALYZER, DYNAMIC ANALYZER, API, DONATE, DOCS, ABOUT, and a SEARCH bar. On the left, a sidebar with various icons provides quick access to different features.

**APP SCORES:** Security Score 56/100, Trackers Detection 0/432, MobSF Scorecard.

**FILE INFORMATION:** File Name: igoat\_ios.zip, Size: 13.68MB, MD5: e018146bda5d7cb14ab45e7f265de8bd, SHA1: 89a8e8cfcd6f1c543ef4b2fe10c505ef404ac9, SHA256: 7e13dedd867e8023fd2cacdc84852917da73f94e6d5fd7cc480cdd7fb, 8418f1a.

**APP INFORMATION:** App Name: iGoat, App Type: Objective-C, Identifier: com.swaroopsy.iGoat, SDK Name: Version: 1.0, Build: 1, Platform Version: Min OS Version, Supported Platforms.

**SCAN OPTIONS:** Buttons for Rescan, Manage Suppressions, View Info.plist, Scan Logs, and Download ZIP.

**CUSTOM URL SCHEMES:** No URL Schemes found.

**APPLICATION PERMISSIONS:** No Permissions required.

## 5. Summary of Vulnerabilities

App Name	High Risk	Medium	Low	Notes
allsafe.apk	2	2	1	Exported activity, hardcoded API key
dvba_v1.1.0.apk	3	3	2	Cleartext traffic, hardcoded secrets, exported activities
insecurebankv2.apk	4	2	1	Debuggable APK, hardcoded credentials, logs, unencrypted DB
iGoat (iOS)	2	1	2	ATS disabled, hardcoded credentials

## 6. Recommendations

## **Android:**

- Remove hardcoded secrets
- Disable debug mode for release builds
- Encrypt local databases
- Use HTTPS for API calls

## **iOS:**

- Enable App Transport Security (ATS)
  - Validate SSL certificates properly
  - Avoid hardcoded credentials
  - Encrypt sensitive local storage
- 

## **7. Conclusion**

The static analysis shows that all tested applications contain security flaws to varying degrees. iGoat intentionally contains vulnerabilities for learning purposes. Android apps also exhibit common security issues such as insecure storage, hardcoded secrets, debug mode enabled, and misconfigured components. Proper fixes are recommended before production deployment.

---