# IOS STATIC ANALYSIS REPORT

No icon

 BitbarIOSSample (1.0)

| File Name: | bitbar-ios-sample.ipa |
| Identifier: | com.bitbar.testdroid.BitbarIOSSample |
| Scan Date: | April 19, 2025, 7:05 a.m. |

| App Security Score: | **67/100 (LOW RISK)** |

| Grade: | **A** |

# ⬤ FINDINGS SEVERITY

| 🐞 HIGH | ⚠ MEDIUM | ℹ INFO | ✔ SECURE | 🔍 HOTSPOT |
|---|---|---|---|---|
| 0 | 3 | 0 | 1 | 0 |

# 📦 FILE INFORMATION

**File Name:** bitbar-ios-sample.ipa
**Size:** 0.14MB
**MD5:** e1f08f17e868e9de32a87d0bdc522fac
**SHA1:** deca43e3dd1186d002dea64b4cef4c8b88142488
**SHA256:** 07ff7a6608265fff57bd3369fb4e10321d939de5101bd966677cd9a210b820b1

# ℹ APP INFORMATION

**App Name:** BitbarIOSSample
**App Type:** Objective C
**Identifier:** com.bitbar.testdroid.BitbarIOSSample
**SDK Name:** iphoneos9.1
**Version:** 1.0
**Build:** 1.0
**Platform Version:** 9.1
**Min OS Version:** 6.0
**Supported Platforms:** iPhoneOS,

# **Ad** BINARY INFORMATION

**Arch:** ARM
**Sub Arch:** CPU_SUBTYPE_ARM_V7
**Bit:** 32-bit
**Endian:** <

# 🔒 APP TRANSPORT SECURITY (ATS)

| NO | ISSUE | SEVERITY | DESCRIPTION |
|----|-------|----------|-------------|
|    |       |          |             |

# </> IPA BINARY CODE ANALYSIS

**HIGH: 0** | **WARNING: 2** | **INFO: 0** | **SECURE: 0** | SUPPRESSED: **0**

| NO | ISSUE | SEVERITY | STANDARDS | DESCRIPTION |
|----|-------|----------|-----------|-------------|
| 1 | Binary makes use of insecure API(s) | warning | **CWE:** CWE-676: Use of Potentially Dangerous Function<br>**OWASP Top 10:** M7: Client Code Quality<br>**OWASP MASVS:** MSTG-CODE-8 | The binary may contain the following insecure API(s) _memcpy , _strlen |
| 2 | Binary makes use of malloc function | warning | **CWE:** CWE-789: Uncontrolled Memory Allocation<br>**OWASP Top 10:** M7: Client Code Quality<br>**OWASP MASVS:** MSTG-CODE-8 | The binary may use _malloc function instead of calloc |

# ⠿ IPA BINARY ANALYSIS

| PROTECTION | STATUS | SEVERITY | DESCRIPTION |
|---|---|---|---|
| NX | 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 always enabled for all third-party code. |
| PIE | True | info | The binary is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably. |
| STACK CANARY | True | info | 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. |
| ARC | False | warning | This binary has debug symbols stripped. We cannot identify whether ARC is enabled or not. |
| RPATH | False | info | The binary does not have Runpath Search Path (@rpath) set. |
| CODE SIGNATURE | True | info | This binary has a code signature. |
| ENCRYPTED | False | warning | This binary is not encrypted. |
| SYMBOLS STRIPPED | True | info | Debug Symbols are stripped |

# </> CODE ANALYSIS

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|-------|----------|-----------|-------|

# ❗ OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

| DOMAIN | COUNTRY/REGION |
|--------|----------------|

# 🔍 DOMAIN MALWARE CHECK

| DOMAIN | STATUS | GEOLOCATION |
|--------|--------|-------------|
| www.apple.com | ok | **IP:** 23.201.200.214<br>**Country:** India<br>**Region:** Maharashtra<br>**City:** Mumbai<br>**Latitude:** 19.014410<br>**Longitude:** 72.847939<br>**View:** Google Map |
| developer.apple.com | ok | **IP:** 17.253.18.201<br>**Country:** Brazil<br>**Region:** Sao Paulo<br>**City:** Sao Paulo<br>**Latitude:** -23.547501<br>**Longitude:** -46.636108<br>**View:** Google Map |

# ≣ SCAN LOGS

| Timestamp | Event | Error |
|---|---|---|
| 2025-04-19 07:05:58 | iOS Binary (IPA) Analysis Started | OK |
| 2025-04-19 07:05:58 | Generating Hashes | OK |
| 2025-04-19 07:05:58 | Extracting IPA | OK |
| 2025-04-19 07:05:58 | Unzipping | OK |
| 2025-04-19 07:05:58 | iOS File Analysis and Normalization | OK |
| 2025-04-19 07:05:59 | iOS Info.plist Analysis Started | OK |
| 2025-04-19 07:05:59 | Finding Info.plist in iOS Binary | OK |
| 2025-04-19 07:05:59 | Fetching Details from App Store: com.bitbar.testdroid.BitbarIOSSample | OK |
| 2025-04-19 07:05:59 | Searching for secrets in plist files | OK |

| 2025-04-19 07:05:59 | Starting Binary Analysis | OK |
|---|---|---|
| 2025-04-19 07:05:59 | Dumping Classes from the binary | OK |
| 2025-04-19 07:05:59 | Running jtool against the binary for dumping classes | OK |
| 2025-04-19 07:05:59 | Library Binary Analysis Started | OK |
| 2025-04-19 07:05:59 | Framework Binary Analysis Started | OK |
| 2025-04-19 07:05:59 | Extracting String Metadata | OK |
| 2025-04-19 07:05:59 | Extracting URL and Email from IPA | OK |
| 2025-04-19 07:05:59 | Performing Malware check on extracted domains | OK |
| 2025-04-19 07:06:00 | Fetching IPA icon path | OK |
| 2025-04-19 07:06:02 | Updating Trackers Database.... | OK |
| 2025-04-19 07:06:02 | Detecting Trackers from Domains | OK |

| 2025-04-19 07:06:02 | Saving to Database | OK |
| --- | --- | --- |

---

## Report Generated by - MobSF v4.3.1

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.