# ANDROID STATIC ANALYSIS REPORT

app_icon

## Allsafe (1.5)

| | |
|---|---|
| File Name: | allsafe.apk |
| Package Name: | infosecadventures.allsafe |
| Scan Date: | Dec. 20, 2025, 6:46 p.m. |
| App Security Score: | 49/100 (MEDIUM RISK) |
| Grade: | B |

# FINDINGS SEVERITY

| HIGH | MEDIUM | INFO | SECURE | HOTSPOT |
|---|---|---|---|---|
| 6 | 16 | 2 | 4 | 1 |

# 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

# APP COMPONENTS

**Activities:** 4
**Services:** 2
**Receivers:** 2
**Providers:** 4
**Exported Activities:** 2
**Exported Services:** 1
**Exported Receivers:** 2
**Exported Providers:** 1

# CERTIFICATE INFORMATION

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

| PERMISSION | STATUS | INFO | DESCRIPTION |
| --- | --- | --- | --- |
| android.permission.INTERNET | normal | full Internet access | Allows an application to create network sockets. |
| 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. |
| android.permission.READ_EXTERNAL_STORAGE | dangerous | read external storage contents | Allows an application to read from external storage. |
| android.permission.WRITE_EXTERNAL_STORAGE | dangerous | read/modify/delete external storage contents | Allows an application to write to external storage. |
| 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 |

# APKID ANALYSIS

| FILE | DETAILS |
| --- | --- |
| classes6.dex | FINDINGS: Compiler — DETAILS: r8 |

| FILE | DETAILS |
| --- | --- |
| classes5.dex | FINDINGS: Compiler — DETAILS: r8 |
| classes3.dex | FINDINGS: Compiler — DETAILS: r8 |
| lib/armeabi-v7a/libtool-checker.so | FINDINGS: anti_root — DETAILS: RootBeer |
| lib/x86_64/libtool-checker.so | FINDINGS: anti_root — DETAILS: RootBeer |
| classes2.dex | FINDINGS: Compiler — DETAILS: unknown (please file detection issue!) |

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>anti_root</td><td>RootBeer</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>lib/x86/libtool-checker.so</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>anti_root</td><td>RootBeer</td></tr>
</table>
</td></tr>
<tr><td>classes7.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.TAGS check<br>possible ro.secure check</td></tr>
<tr><td>anti_root</td><td>RootBeer</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

| FILE | DETAILS |
| --- | --- |
| classes.dex | <table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check<br>Build.MODEL check<br>Build.MANUFACTURER check<br>Build.BRAND check</td></tr><tr><td>Compiler</td><td>r8</td></tr></table> |

# BROWSABLE ACTIVITIES

| ACTIVITY | INTENT |
| --- | --- |
| infosecadventures.allsafe.challenges.DeepLinkTask | Schemes: allsafe://, https://,<br>Hosts: infosecadventures,<br>Path Prefixes: /congrats, |

# NETWORK SECURITY

HIGH: **1** | WARNING: **0** | INFO: **0** | SECURE: **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

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

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. |

| NO | ISSUE | SEVERITY | DESCRIPTION |
|---|---|---|---|
| 4 | Application Data can be Backed up<br>[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.<br>[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.<br>[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.<br>[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.<br>[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.<br>[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.<br>Permission: android.permission.DUMP<br>[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. |

# CODE ANALYSIS

HIGH: 1 | WARNING: 6 | INFO: 2 | SECURE: 2 | SUPPRESSED: 0

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 1 | The App logs information. Sensitive information should never be logged. | info | CWE: CWE-532: Insertion of Sensitive Information into Log File<br>OWASP MASVS: MSTG-STORAGE-3 | com/scottyab/rootbeer/RootBeer.java<br>com/scottyab/rootbeer/RootBeerNative.java<br>com/scottyab/rootbeer/util/QLog.java<br>infosecadventures/allsafe/challenges/CertificatePinning.java<br>infosecadventures/allsafe/challenges/DeepLinkTask.java<br>infosecadventures/allsafe/challenges/InsecureLogging.java<br>infosecadventures/allsafe/challenges/NoteReceiver.java<br>infosecadventures/allsafe/challenges/ObjectSerialization.java<br>infosecadventures/allsafe/challenges/RecorderService.java<br>infosecadventures/allsafe/challenges/WeakCryptography.java |
| 2 | App can read/write to External Storage. Any App can read data written to External Storage. | warning | CWE: CWE-276: Incorrect Default Permissions<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2 | infosecadventures/allsafe/challenges/ObjectSerialization.java<br>infosecadventures/allsafe/challenges/RecorderService.java |
| 3 | This App may request root (Super User) privileges. | warning | CWE: CWE-250: Execution with Unnecessary Privileges<br>OWASP MASVS: MSTG-RESILIENCE-1 | com/scottyab/rootbeer/Const.java |
| 4 | App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database. | warning | CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')<br>OWASP Top 10: M7: Client Code Quality | infosecadventures/allsafe/challenges/NoteDatabaseHelper.java<br>infosecadventures/allsafe/challenges/SQLInjection.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 5 | MD5 is a weak hash known to have hash collisions. | warning | CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-4 | infosecadventures/allsafe/challenges/SQLInjection.java<br>infosecadventures/allsafe/challenges/WeakCryptography.java |
| 6 | Files may contain hardcoded sensitive information like usernames, passwords, keys etc. | warning | CWE: CWE-312: Cleartext Storage of Sensitive Information<br>OWASP Top 10: M9: Reverse Engineering<br>OWASP MASVS: MSTG-STORAGE-14 | infosecadventures/allsafe/challenges/ObjectSerialization.java<br>infosecadventures/allsafe/challenges/SQLInjection.java<br>infosecadventures/allsafe/challenges/WeakCryptography.java |
| 7 | This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel. | secure | OWASP MASVS: MSTG-NETWORK-4 | infosecadventures/allsafe/challenges/CertificatePinning.java |
| 8 | This App may have root detection capabilities. | secure | OWASP MASVS: MSTG-RESILIENCE-1 | com/scottyab/rootbeer/RootBeer.java |
| 9 | This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it. | info | OWASP MASVS: MSTG-STORAGE-10 | infosecadventures/allsafe/utils/ClipUtil.java |
| 10 | The App uses an insecure Random Number Generator. | warning | CWE: CWE-330: Use of Insufficiently Random Values<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-6 | infosecadventures/allsafe/challenges/WeakCryptography.java |
| 11 | The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext. | high | CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-2 | infosecadventures/allsafe/challenges/WeakCryptography.java |

# SHARED LIBRARY BINARY ANALYSIS

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|---|
| 1 | armeabi-v7a/libtool-checker.so | True<br>info<br>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | Dynamic Shared Object (DSO)<br>info<br>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably. | True<br>info<br>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. | Full RELRO<br>info<br>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only. | None<br>info<br>The binary does not have run-time search path or RPATH set. | None<br>info<br>The binary does not have RUNPATH set. | False<br>warning<br>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries. | True<br>info<br>Symbols are stripped. |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|---|
| 2 | armeabi-v7a/libnative_library.so | True<br>info<br>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | Dynamic Shared Object (DSO)<br>info<br>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably. | True<br>info<br>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. | Full RELRO<br>info<br>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only. | None<br>info<br>The binary does not have run-time search path or RPATH set. | None<br>info<br>The binary does not have RUNPATH set. | True<br>info<br>The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk'] | True<br>info<br>Symbols are stripped. |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|---|
| 3 | x86/libtool-checker.so | True<br>info<br>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | Dynamic Shared Object (DSO)<br>info<br>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably. | True<br>info<br>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. | Full RELRO<br>info<br>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only. | None<br>info<br>The binary does not have run-time search path or RPATH set. | None<br>info<br>The binary does not have RUNPATH set. | False<br>warning<br>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries. | True<br>info<br>Symbols are stripped. |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|---|
| 4 | x86/libnative_library.so | True<br>info<br>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | Dynamic Shared Object (DSO)<br>info<br>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably. | True<br>info<br>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. | Full RELRO<br>info<br>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only. | None<br>info<br>The binary does not have run-time search path or RPATH set. | None<br>info<br>The binary does not have RUNPATH set. | True<br>info<br>The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk'] | True<br>info<br>Symbols are stripped. |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|---|
| 5 | arm64-v8a/libtool-checker.so | True<br>info<br>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | Dynamic Shared Object (DSO)<br>info<br>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably. | False<br>high<br>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. Not applicable for Dart/Flutter libraries unless Dart FFI is used. | Full RELRO<br>info<br>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only. | None<br>info<br>The binary does not have run-time search path or RPATH set. | None<br>info<br>The binary does not have RUNPATH set. | False<br>warning<br>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries. | True<br>info<br>Symbols are stripped. |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|---|
| 6 | arm64-v8a/libnative_library.so | True<br>info<br>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | Dynamic Shared Object (DSO)<br>info<br>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably. | True<br>info<br>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. | Full RELRO<br>info<br>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only. | None<br>info<br>The binary does not have run-time search path or RPATH set. | None<br>info<br>The binary does not have RUNPATH set. | True<br>info<br>The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk'] | True<br>info<br>Symbols are stripped. |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|---|
| 7 | x86_64/libtool-checker.so | True<br>info<br>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | Dynamic Shared Object (DSO)<br>info<br>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably. | False<br>high<br>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. Not applicable for Dart/Flutter libraries unless Dart FFI is used. | Full RELRO<br>info<br>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only. | None<br>info<br>The binary does not have run-time search path or RPATH set. | None<br>info<br>The binary does not have RUNPATH set. | False<br>warning<br>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries. | True<br>info<br>Symbols are stripped. |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|---|
| 8 | x86_64/libnative_library.so | True<br>info<br>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | Dynamic Shared Object (DSO)<br>info<br>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably. | True<br>info<br>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. | Full RELRO<br>info<br>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only. | None<br>info<br>The binary does not have run-time search path or RPATH set. | None<br>info<br>The binary does not have RUNPATH set. | True<br>info<br>The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk'] | True<br>info<br>Symbols are stripped. |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|---|
| 9 | armeabi-v7a/libtool-checker.so | True<br>info<br>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | Dynamic Shared Object (DSO)<br>info<br>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably. | True<br>info<br>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. | Full RELRO<br>info<br>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only. | None<br>info<br>The binary does not have run-time search path or RPATH set. | None<br>info<br>The binary does not have RUNPATH set. | False<br>warning<br>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries. | True<br>info<br>Symbols are stripped. |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|---|
| 10 | armeabi-v7a/libnative_library.so | True<br>info<br>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | Dynamic Shared Object (DSO)<br>info<br>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably. | True<br>info<br>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. | Full RELRO<br>info<br>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only. | None<br>info<br>The binary does not have run-time search path or RPATH set. | None<br>info<br>The binary does not have RUNPATH set. | True<br>info<br>The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk'] | True<br>info<br>Symbols are stripped. |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|---|
| 11 | x86/libtool-checker.so | True<br>info<br>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | Dynamic Shared Object (DSO)<br>info<br>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably. | True<br>info<br>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. | Full RELRO<br>info<br>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only. | None<br>info<br>The binary does not have run-time search path or RPATH set. | None<br>info<br>The binary does not have RUNPATH set. | False<br>warning<br>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries. | True<br>info<br>Symbols are stripped. |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|---|
| 12 | x86/libnative_library.so | True<br>info<br>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | Dynamic Shared Object (DSO)<br>info<br>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably. | True<br>info<br>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. | Full RELRO<br>info<br>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only. | None<br>info<br>The binary does not have run-time search path or RPATH set. | None<br>info<br>The binary does not have RUNPATH set. | True<br>info<br>The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk'] | True<br>info<br>Symbols are stripped. |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|---|
| 13 | arm64-v8a/libtool-checker.so | True<br>info<br>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | Dynamic Shared Object (DSO)<br>info<br>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably. | False<br>high<br>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. Not applicable for Dart/Flutter libraries unless Dart FFI is used. | Full RELRO<br>info<br>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only. | None<br>info<br>The binary does not have run-time search path or RPATH set. | None<br>info<br>The binary does not have RUNPATH set. | False<br>warning<br>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries. | True<br>info<br>Symbols are stripped. |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|---|
| 14 | arm64-v8a/libnative_library.so | True<br>info<br>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | Dynamic Shared Object (DSO)<br>info<br>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably. | True<br>info<br>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. | Full RELRO<br>info<br>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only. | None<br>info<br>The binary does not have run-time search path or RPATH set. | None<br>info<br>The binary does not have RUNPATH set. | True<br>info<br>The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk'] | True<br>info<br>Symbols are stripped. |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|---|
| 15 | x86_64/libtool-checker.so | True<br>info<br>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | Dynamic Shared Object (DSO)<br>info<br>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably. | False<br>high<br>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. Not applicable for Dart/Flutter libraries unless Dart FFI is used. | Full RELRO<br>info<br>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only. | None<br>info<br>The binary does not have run-time search path or RPATH set. | None<br>info<br>The binary does not have RUNPATH set. | False<br>warning<br>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries. | True<br>info<br>Symbols are stripped. |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|---|
| 16 | x86_64/libnative_library.so | True<br>info<br>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | Dynamic Shared Object (DSO)<br>info<br>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably. | True<br>info<br>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. | Full RELRO<br>info<br>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only. | None<br>info<br>The binary does not have run-time search path or RPATH set. | None<br>info<br>The binary does not have RUNPATH set. | True<br>info<br>The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk'] | True<br>info<br>Symbols are stripped. |

# NIAP ANALYSIS v1.3

| NO | IDENTIFIER | REQUIREMENT | FEATURE | DESCRIPTION |
|---|---|---|---|---|

# BEHAVIOUR ANALYSIS

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---|---|---|---|
| 00022 | Open a file from given absolute path of the file | file | infosecadventures/allsafe/ArbitraryCodeExecution.java<br>infosecadventures/allsafe/challenges/InsecureProviders.java<br>infosecadventures/allsafe/challenges/RecorderService.java |
| 00195 | Set the output path of the recorded file | record file | infosecadventures/allsafe/challenges/RecorderService.java |
| 00199 | Stop recording and release recording resources | record | infosecadventures/allsafe/challenges/RecorderService.java |
| 00198 | Initialize the recorder and start recording | record | infosecadventures/allsafe/challenges/RecorderService.java |
| 00194 | Set the audio source (MIC) and recorded file format | record | infosecadventures/allsafe/challenges/RecorderService.java |
| 00197 | Set the audio encoder and initialize the recorder | record | infosecadventures/allsafe/challenges/RecorderService.java |
| 00007 | Use absolute path of directory for the output media file path | file | infosecadventures/allsafe/challenges/RecorderService.java |
| 00196 | Set the recorded file format and output path | record file | infosecadventures/allsafe/challenges/RecorderService.java |
| 00013 | Read file and put it into a stream | file | infosecadventures/allsafe/challenges/ObjectSerialization.java<br>okio/Okio__JvmOkioKt.java |
| 00063 | Implicit intent(view a web page, make a phone call, etc.) | control | infosecadventures/allsafe/about/About.java |

# FIREBASE DATABASES ANALYSIS

| TITLE | SEVERITY | DESCRIPTION |
|---|---|---|
| Open Firebase database | high | The Firebase database at https://allsafe-8cef0.firebaseio.com/.json is exposed to internet without any authentication |
| 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'} |

# ABUSED PERMISSIONS

| TYPE | MATCHES | PERMISSIONS |
|---|---|---|
| Malware Permissions | 5/25 | android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.RECORD_AUDIO, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE |
| Other Common Permissions | 0/44 | |

### Malware Permissions:
Top permissions that are widely abused by known malware.
### Other Common Permissions:
Permissions that are commonly abused by known malware.

# OFAC SANCTIONED COUNTRIES

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

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

# DOMAIN MALWARE CHECK

| DOMAIN | STATUS | GEOLOCATION |
| --- | --- | --- |
| httpbin.io | ok | **IP:** 52.70.33.41<br>**Country:** United States of America<br>**Region:** Virginia<br>**City:** Ashburn<br>**Latitude:** 39.043720<br>**Longitude:** -77.487488<br>**View:** Google Map |
| dev.infosecadventures.com | ok | No Geolocation information available. |
| allsafe-8cef0.firebaseio.com | ok | **IP:** 35.190.39.113<br>**Country:** United States of America<br>**Region:** Missouri<br>**City:** Kansas City<br>**Latitude:** 39.099731<br>**Longitude:** -94.578568<br>**View:** Google Map |
| schemas.xmlsoap.org | ok | **IP:** 13.107.213.53<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Redmond<br>**Latitude:** 47.682899<br>**Longitude:** -122.120903<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
| --- | --- | --- |
| medium.com | ok | **IP:** 162.159.153.4<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| www.github.com | ok | **IP:** 140.82.121.4<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| www.x.com | ok | **IP:** 162.159.140.229<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| siebel.com | ok | **IP:** 92.123.104.20<br>**Country:** Germany<br>**Region:** Hessen<br>**City:** Frankfurt am Main<br>**Latitude:** 50.115520<br>**Longitude:** 8.684170<br>**View:** Google Map |

## EMAILS

| EMAIL | FILE |
| --- | --- |
| password123@dev.infosecadv | Android String Resource |

# HARDCODED SECRETS

| POSSIBLE 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" |
| 0af58729667eace3883a992ef2b8ce29 |
| aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7 |
| 23456789abcdefghjkmnpqrstvwxyz |
| 3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112319 |
| 1157920892103562487626974469494075735300861434152903141955336313088670978539 51 |
| 6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449 |
| 65dc3431f8c5e3f0e249c5b1c6e3534d |
| 3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3 |

| POSSIBLE SECRETS |
| --- |
| 11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650 |
| 6d2e1c6dd505a108cc7e19a46aa30a8a |
| 1835a58E866a668C48Ee63d32432C7Fe28aF54b4 |
| 4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5 |
| bc1qd44kvj6zatjgn27n45uxd3nprzt6rm9x9g2yc8 |
| d510b80eb22f8eb684f1a19681eb7bcf |
| 051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00 |
| 3484cef7f6ff172c2cd278d3b51f3e66 |
| 21232f297a57a5a743894a0e4a801fc3 |
| 6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151 |
| b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef |
| c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66 |
| 1157920892103562487626974469494075735299969552241357603424222590610685120443 69 |
| 6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296 |
| 5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b |
| 3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f |

| POSSIBLE SECRETS |
| --- |
| 258EAFA5-E914-47DA-95CA-C5AB0DC85B11 |

## SCAN LOGS

| Timestamp | Event | Error |
| --- | --- | --- |
| 2025-12-20 19:01:31 | Generating Hashes | OK |
| 2025-12-20 19:01:31 | Extracting APK | OK |
| 2025-12-20 19:01:31 | Unzipping | OK |
| 2025-12-20 19:01:32 | Parsing APK with androguard | OK |
| 2025-12-20 19:01:32 | Extracting APK features using aapt/aapt2 | OK |
| 2025-12-20 19:01:32 | Getting Hardcoded Certificates/Keystores | OK |
| 2025-12-20 19:01:36 | Parsing AndroidManifest.xml | OK |
| 2025-12-20 19:01:36 | Extracting Manifest Data | OK |

| | | |
|---|---|---|
| 2025-12-20 19:01:36 | Manifest Analysis Started | OK |
| 2025-12-20 19:01:36 | Reading Network Security config from network_security_config.xml | OK |
| 2025-12-20 19:01:36 | Parsing Network Security config | OK |
| 2025-12-20 19:01:36 | Performing Static Analysis on: Allsafe (infosecadventures.allsafe) | OK |
| 2025-12-20 19:01:36 | Fetching Details from Play Store: infosecadventures.allsafe | OK |
| 2025-12-20 19:01:36 | Checking for Malware Permissions | OK |
| 2025-12-20 19:01:36 | Fetching icon path | OK |
| 2025-12-20 19:01:36 | Library Binary Analysis Started | OK |
| 2025-12-20 19:01:36 | Analyzing lib/armeabi-v7a/libtool-checker.so | OK |
| 2025-12-20 19:01:36 | Analyzing lib/armeabi-v7a/libnative_library.so | OK |
| 2025-12-20 19:01:37 | Analyzing lib/x86/libtool-checker.so | OK |

| | | |
|---|---|---|
| 2025-12-20 19:01:37 | Analyzing lib/x86/libnative_library.so | OK |
| 2025-12-20 19:01:37 | Analyzing lib/arm64-v8a/libtool-checker.so | OK |
| 2025-12-20 19:01:37 | Analyzing lib/arm64-v8a/libnative_library.so | OK |
| 2025-12-20 19:01:37 | Analyzing lib/x86_64/libtool-checker.so | OK |
| 2025-12-20 19:01:37 | Analyzing lib/x86_64/libnative_library.so | OK |
| 2025-12-20 19:01:37 | Analyzing apktool_out/lib/armeabi-v7a/libtool-checker.so | OK |
| 2025-12-20 19:01:37 | Analyzing apktool_out/lib/armeabi-v7a/libnative_library.so | OK |
| 2025-12-20 19:01:37 | Analyzing apktool_out/lib/x86/libtool-checker.so | OK |
| 2025-12-20 19:01:37 | Analyzing apktool_out/lib/x86/libnative_library.so | OK |
| 2025-12-20 19:01:37 | Analyzing apktool_out/lib/arm64-v8a/libtool-checker.so | OK |
| 2025-12-20 19:01:37 | Analyzing apktool_out/lib/arm64-v8a/libnative_library.so | OK |

| | | |
|---|---|---|
| 2025-12-20 19:01:37 | Analyzing apktool_out/lib/x86_64/libtool-checker.so | OK |
| 2025-12-20 19:01:37 | Analyzing apktool_out/lib/x86_64/libnative_library.so | OK |
| 2025-12-20 19:01:37 | Reading Code Signing Certificate | OK |
| 2025-12-20 19:01:38 | Running APKiD 3.0.0 | OK |
| 2025-12-20 19:01:42 | Detecting Trackers | OK |
| 2025-12-20 19:01:47 | Decompiling APK to Java with JADX | OK |
| 2025-12-20 19:02:32 | Converting DEX to Smali | OK |
| 2025-12-20 19:02:33 | Code Analysis Started on - java_source | OK |
| 2025-12-20 19:02:34 | Android SBOM Analysis Completed | OK |
| 2025-12-20 19:02:46 | Android SAST Completed | OK |
| 2025-12-20 19:02:46 | Android API Analysis Started | OK |

| | | |
|---|---|---|
| 2025-12-20 19:02:52 | Android API Analysis Completed | OK |
| 2025-12-20 19:02:52 | Android Permission Mapping Started | OK |
| 2025-12-20 19:03:28 | Android Permission Mapping Completed | OK |
| 2025-12-20 19:03:29 | Android Behaviour Analysis Started | OK |
| 2025-12-20 19:03:35 | Android Behaviour Analysis Completed | OK |
| 2025-12-20 19:03:35 | Extracting Emails and URLs from Source Code | OK |
| 2025-12-20 19:03:36 | Email and URL Extraction Completed | OK |
| 2025-12-20 19:03:36 | Extracting String data from APK | OK |
| 2025-12-20 19:03:36 | Extracting String data from SO | OK |
| 2025-12-20 19:03:36 | Extracting String data from Code | OK |
| 2025-12-20 19:03:36 | Extracting String values and entropies from Code | OK |

| | | |
|---|---|---|
| 2025-12-20 19:03:40 | Performing Malware check on extracted domains | OK |
| 2025-12-20 19:03:42 | Saving to Database | OK |

---

## Report Generated by - MobSF v4.4.4

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.