MOBSF

ANDROID STATIC ANALYSIS REPORT

SBI_ONLINE_KYC_.apk (Failed)

File Name:	SBI_ONLINE_KYC_.apk
Package Name:	Failed
Scan Date:	Nov. 14, 2025, 1:51 p.m.
App Security Score:	44/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	2	1	1	0

FILE INFORMATION

File Name: SBI_ONLINE_KYC_.apk
Size: 3.93MB
MD5: 5227f62d7ed76684cc3e9e754ad3720e
SHA1: 9f22e72ca7758e2cacc92c7e43617c55dbf5fd3e
SHA256: f23bd40dfb289fd10017e6924432b2cfcf8523811dafc2ad890fcada2da5a59d

APP INFORMATION

App Name:
Package Name: Failed
Main Activity:
Target SDK:
Min SDK:
Max SDK:
Android Version Name: Failed
Android Version Code: Failed

APP COMPONENTS

Activities: 0
Services: 0
Receivers: 0
Providers: 0
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: None
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google, OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2025-10-20 03:49:06+00:00
Valid To: 2035-10-18 03:49:06+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google, OU=Android, CN=Android
Serial Number: 0x9f4a657625820628
Hash Algorithm: md5
md5: ffe93a084996fe6ca67fb9969648f612
sha1: 28fc51e707a44ca7b84392a08facaf556bcba0a0
sha256: cb3c97c5d4ff4dbb7bb31203e837ea1b6a0573e3ae05ed1a3a0771aa18c87843
sha512: 0dd301e370327c0648c9b037d3f9e5689cdf82a4f9c6825f8355e83b1ed71a2847915b2b988a90c2ece8360b2501de5d1bff5a95ea6c72872ca30db67785b4cd
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 1f6c42369f9699bd9e4993937414c049e1afb899474f1003a94bf3f1b71f84b8
Found 1 unique certificates

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>□
□□.temp!classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Obfuscator</td><td>unreadable field names
unreadable method names</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>Obfuscator</td><td>unreadable field names
unreadable method names</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm vulnerable to hash collision	high	Application is signed with MD5. MD5 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION

CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				A/c.java B/b.java B/j.java B/o.java

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 OWASP MASVS: MSTG-STORAGE-3	B/r.java B0/t.java B0/q.java C/g.java C/h.java C/i.java C/j.java C/k.java E0/d.java F0/a.java G/g.java H/a.java H/b.java H/d.java H0/e.java H0/g.java K/C0059b.java K/C0071n.java K/F.java K/Q.java K/V.java K/l0.java K/m0.java K/q0.java K0/k.java Q/t.java S/e.java U/C0017.java U/g.java W/d.java W0/C0019.java b0/AbstractC0130f.java d0/C0162v.java d0/I.java d0/S.java d0/X.java e/AbstractActivityC0175h.java e/n.java e/p.java e/v.java e/z.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				h/C0190g.java h/C0191h.java i/ViewOnKeyListenerC0230g.java a i/m.java i0/p.java j/AbstractC0246c0.java j/C0254g0.java j/C0280u.java j/C0284w.java j/E0.java j/J0.java j/K.java j/Q.java j/Q0.java j/f1.java n0/C0308b.java p/C0047.java q/C0322c.java s/C0333e.java v/b.java v/f.java v/i.java v/m.java z/b.java z/d.java
2	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	B/o.java V0/a.java V0/b.java V0/c.java W0/a.java
3	The file or SharedPreference is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	J0/C0011.java
4	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	B0/q.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	A/c.java B/o.java B0/q.java C/i.java C/j.java b0/AbstractC0130f.java b0/C0126b.java b0/C0136l.java z/d.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	e/w.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	e/w.java
00036	Get resource file from res/raw directory	reflection	e/w.java
00147	Get the time of current location	collection location	e/v.java
00075	Get location of the device	collection location	e/v.java

RULE ID	BEHAVIOUR	LABEL	FILES
00115	Get last known location of the device	collection location	e/v.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	0/25	
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
schemas.android.com	ok	No Geolocation information available.

HARDCODED SECRETS

POSSIBLE SECRETS
RmFpbGVkIHRvIHByZXBhcmUgdXBkYXRlLiBQbGVhc2UgdHJ5IGFnYWluLg==

SCAN LOGS

Timestamp	Event	Error
2025-11-14 13:51:37	Generating Hashes	OK
2025-11-14 13:51:37	Extracting APK	OK
2025-11-14 13:51:37	Unzipping	OK
2025-11-14 13:51:38	Parsing APK with androguard	OK

2025-11-14 13:51:38	Failed to parse AndroidManifest.xml with androguard	AttributeError("'NoneType' object has no attribute 'get_xml'")
2025-11-14 13:51:38	Extracting APK features using aapt/aapt2	OK
2025-11-14 13:51:38	Getting Hardcoded Certificates/Keystores	OK
2025-11-14 13:51:40	Failed to extract AndroidManifest.xml from APK with apktool and androguard	apktool and androguard failed
2025-11-14 13:51:40	Extracting Manifest Data	OK
2025-11-14 13:51:40	Manifest Analysis Started	OK
2025-11-14 13:51:40	Performing Static Analysis on: Failed	OK
2025-11-14 13:51:42	Fetching Details from Play Store: Failed	OK
2025-11-14 13:51:42	Checking for Malware Permissions	OK
2025-11-14 13:51:42	Fetching icon path	OK

2025-11-14 13:51:42	Library Binary Analysis Started	OK
2025-11-14 13:51:42	Reading Code Signing Certificate	OK
2025-11-14 13:51:43	Failed to get signature versions with apksigner	CalledProcessError(1, ['/jdk-22.0.2/bin/java', '-Xmx1024M', '-Djava.library.path=', '-jar', '/home/mobsf/Mobile-Security-Framework-MobSF/mobsf/StaticAnalyzer/tools/apksigner.jar', 'verify', '--verbose', '/home/mobsf/.MobSF/uploads/5227f62d7ed76684cc3e9e754ad3720e/5227f62d7ed76684cc3e9e754ad3720e.apk'])
2025-11-14 13:51:43	Running APKiD 3.0.0	OK
2025-11-14 13:51:47	Detecting Trackers	OK
2025-11-14 13:51:47	Decompiling APK to Java with JADX	OK
2025-11-14 13:51:50	Decompiling with JADX failed, attempting on all DEX files	OK
2025-11-14 13:51:50	Decompiling classes.dex with JADX	OK
2025-11-14 13:51:59	Converting DEX to Smali	OK
2025-11-14 13:51:59	Code Analysis Started on - java_source	OK

2025-11-14 13:52:01	Android SBOM Analysis Completed	OK
2025-11-14 13:52:02	Android SAST Completed	OK
2025-11-14 13:52:02	Android API Analysis Started	OK
2025-11-14 13:52:03	Android API Analysis Completed	OK
2025-11-14 13:52:03	Android Behaviour Analysis Started	OK
2025-11-14 13:52:06	Android Behaviour Analysis Completed	OK
2025-11-14 13:52:06	Extracting Emails and URLs from Source Code	OK
2025-11-14 13:52:06	Email and URL Extraction Completed	OK
2025-11-14 13:52:06	Extracting String data from Code	OK
2025-11-14 13:52:06	Extracting String values and entropies from Code	OK

2025-11-14 13:52:07	Performing Malware check on extracted domains	OK
2025-11-14 13:52:11	Saving to Database	OK

Report Generated by - MobSF v4.4.3

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.