MOBSF

ANDROID STATIC ANALYSIS REPORT

JS Mobile (1.0.21.3)

File Name:	JS.apk
Package Name:	com.JSBL.bank
Scan Date:	Oct. 19, 2024, 11:02 a.m.
App Security Score:	49/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	14	2	2	2

FILE INFORMATION

File Name: JS.apk
Size: 46.27MB
MD5: 62166eec872dec8d987e18059d7b1e44
SHA1: 85f7b753874aad459115ea943d24e25c9ae32be8
SHA256: dbdd48dc0072763b9456c899540cf212f3751975bf17c1371373e837fd3c2243

APP INFORMATION

App Name: JS Mobile
Package Name: com.JSBL.bank
Main Activity: com.JSBL.bank.Activities.SUSDF
Target SDK: 34
Min SDK: 23
Max SDK:
Android Version Name: 1.0.21.3

Android Version Code: 62

APP COMPONENTS

Activities: 23
Services: 14
Receivers: 12
Providers: 5
Exported Activities: 1
Exported Services: 1
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-04-06 13:28:36+00:00
Valid To: 2051-04-06 13:28:36+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x6e52ea12b329f46d4a84373bdf9562ccad84acc1
Hash Algorithm: sha256
md5: 71e393972294001d4d37d4faa8c744fc
sha1: b844dd01344c7930b4d82da4e45b868576bf66ec
sha256: 511df77b621453b4247e9ce3c729cd858e8d411a96cb37d9624292f57b5882df
sha512: 39da693fe46f2e09144fc44e4e5a508cdb41fbe92ba3deaaf390643f10b9690dd6a24473cdf2681a728b6328a0944500d28c221a0b05bebac5cf1f3d38a616dc
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: a0683ea3bfcebe40f21d30cea39a3f43368945475657c6efe51e7455b4b627a3
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_PRIVILEGED_PHONE_STATE	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.ACCESS_MEDIA_LOCATION	dangerous	access any geographic locations	Allows an application to access any geographic locations persisted in the user's shared collection.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECEIVE_SMS	dangerous	receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.WRITE_CONTACTS	dangerous	write contact data	Allows an application to modify the contact (address) data stored on your phone. Malicious applications can use this to erase or modify your contact data.
android.permission.READ_PHONE_NUMBERS	dangerous	allows reading of the device's phone number(s).	Allows read access to the device's phone number(s). This is a subset of the capabilities granted by READ_PHONE_STATE but is exposed to instant applications.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></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
Build.TAGS check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
possible ro.secure check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes3.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MANUFACTURER check possible Build.SERIAL check Build.TAGS check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

TITLE	SEVERITY	DESCRIPTION
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.

MANIFEST ANALYSIS

HIGH: **2** | WARNING: **4** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched 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	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, 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.
3	Activity (com.JSBL.bank.Activities.FUASDFPASDF) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [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.
5	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [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. 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.
6	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 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.

</> CODE ANALYSIS

HIGH: 1 | WARNING: 7 | INFO: 2 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES

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	com/bumptech/glide/a.java com/unikrew/faceoff/liveness/b/a.java com/veridiumid/sdk/analytics/AnalyticsLibraryDataDumpInternalUse.java com/veridiumid/sdk/log/Timber.java defpackage/a60.java defpackage/b63.java defpackage/be1.java defpackage/ce3.java defpackage/cp3.java defpackage/d70.java defpackage/eq1.java defpackage/f63.java defpackage/fh0.java defpackage/gd2.java defpackage/hg0.java defpackage/hk.java defpackage/it2.java defpackage/k10.java defpackage/mz0.java defpackage/nj3.java defpackage/ob0.java defpackage/p73.java defpackage/pm2.java defpackage/rd3.java defpackage/ri1.java defpackage/s83.java defpackage/si.java defpackage/si1.java defpackage/t9.java defpackage/ti.java defpackage/tn3.java defpackage/v90.java defpackage/vx.java defpackage/wb0.java defpackage/xe0.java defpackage/y50.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/tensorflow/lite/NativeInterpreterWrapper.java
2	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/veridiumid/sdk/model/help/EncryptionUtils.java
3	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/veridiumid/sdk/internal/licensing/ws/LicensingServiceApi.java defpackage/gd2.java defpackage/hj.java defpackage/hx.java defpackage/r62.java
4	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	com/unikrew/faceoff/fingerprint/SecureStorage/c.java com/unikrew/faceoff/liveness/SecureStorage/c.java
5	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	defpackage/ev2.java defpackage/f52.java defpackage/hm.java defpackage/kd2.java defpackage/lh0.java defpackage/mg0.java defpackage/na0.java defpackage/o0.java defpackage/q92.java defpackage/yy2.java
6	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	defpackage/fx0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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') OWASP Top 10: M7: Client Code Quality	defpackage/ap0.java defpackage/z71.java
8	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/theartofdev/edmodo/cropper/CropImageActivity.java com/theartofdev/edmodo/cropper/CropImageView.java defpackage/hq3.java defpackage/qz2.java
9	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java com/veridiumid/sdk/fourf/camera/FourFCamera2.java defpackage/e23.java defpackage/fa2.java
10	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java com/veridiumid/sdk/defaultdata/securepreferences/SecurePreferences.java defpackage/bf0.java defpackage/e52.java
11	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	com/veridiumid/sdk/model/help/AndroidHelper.java defpackage/jx.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
12	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/veridiumid/sdk/model/help/AndroidHelper.java defpackage/ww2.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	15/24	android.permission.READ_SMS, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_WIFI_STATE, android.permission.CAMERA, android.permission.READ_PHONE_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.RECEIVE_SMS, android.permission.INTERNET, android.permission.VIBRATE, android.permission.READ_CONTACTS, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	5/45	android.permission.WRITE_CONTACTS, android.permission.CHANGE_WIFI_STATE, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.FOREGROUND_SERVICE

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
unikrew-faceoff-licensing.azurewebsites.net	ok	**IP:** 65.52.250.96 **Country:** United Arab Emirates **Region:** Dubayy **City:** Dubai **Latitude:** 25.258169 **Longitude:** 55.304722 **View:** Google Map
jsmbphoenix.jsbl.com	ok	**IP:** 104.19.251.92 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
qa-jsbankmao.appinsnap.com	ok	**IP:** 104.215.249.5 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
unikrewutilsbackend.azurewebsites.net	ok	**IP:** 104.45.1.117 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
facial-spoof-detection2.services-backend.com	ok	**IP:** 172.67.70.49 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
unikrew-faceoff-telemetry.azurewebsites.net	ok	**IP:** 65.52.250.96 **Country:** United Arab Emirates **Region:** Dubayy **City:** Dubai **Latitude:** 25.258169 **Longitude:** 55.304722 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
faceoffmobilebackend.azurewebsites.net	ok	**IP:** 13.77.82.141 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map
github.com	ok	**IP:** 20.207.73.82 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
sindh-vaccine.shelterhomes.pk	ok	No Geolocation information available.
js-mobile-banking.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
play.google.com	ok	**IP:** 142.250.183.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
faceoffauthentication.azurewebsites.net	ok	**IP:** 13.77.82.141 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map
meezan-faceoff-backend.covalent.pk	ok	No Geolocation information available.
jsbl.com	ok	**IP:** 104.19.251.92 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.whatsapp.com	ok	**IP:** 157.240.227.60 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
licensing.prod.veridium-dev.com	ok	**IP:** 3.64.32.202 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ns.adobe.com	ok	No Geolocation information available.
journeyapps.com	ok	**IP:** 108.139.59.90 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
meezan-faceoff-ids.covalent.pk	ok	No Geolocation information available.

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://js-mobile-banking.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
ccu.helpdesk@jsbl.com email@gmail.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://js-mobile-banking.firebaseio.com"
"google_api_key" : "AIzaSyD1I3qMKKzEavxFdoZqRH9TUP6R-XX7q9o"
"google_crash_reporting_api_key" : "AIzaSyD1I3qMKKzEavxFdoZqRH9TUP6R-XX7q9o"
"google_maps_key" : "AIzaSyDXbeduJIII5I3irMmUfCzKKkJQ6YSSJQA"
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"

POSSIBLE SECRETS
"password" : "**********"
sha256/zIFoxgdrRd3vHp23nR+JPrVkfEOXI2xDAQSodOAbPXQ=
sha256/F+w2csaxLrP89+DcS32ktRqk267Am2lWuUR0TM0W7K4=
01360240043788015936020505
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
470fa2b4ae81cd56ecbcda9735803434cec591fa
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
9a04f079-9840-4286-ab92-e65be0885f95
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3

POSSIBLE SECRETS
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
c103703e120ae8cc73c9248622f3cd1e
49f946663a8deb7054212b8adda248c6
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D78
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151

PLAYSTORE INFORMATION

Title: JS Mobile

Score: 3.82 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Finance **Play Store URL:** com.JSBL.bank

Developer Details: JS Bank Limited, 4829726064783917879, Shaheen Commercial Complex Dr. Ziauddin Ahmed Road P.O. Box 4847, Karachi-74200 Sindh, Pakistan,

https://jsbl.com/, jsmb@jsbl.com,

Release Date: Apr 6, 2021 **Privacy Policy:** Privacy link

Description:

Access your JS Bank account instantly, make payments on-the-go and transfer funds to anyone safely and securely with your device. It's fast. It's smooth. It's simple. Mobile banking has never been easier. Salient Features: 1. Get access to your account information in simple steps. 2. View account balance, account statement, and transaction details for all your accounts. 3. Make instant Fund Transfers to JS Bank and other IBFT enabled Bank customers. 4. Pay your utility bills on-the-go. 5. Locate your nearest JS Bank branches and ATMs. Download Now! For further assistance, you can reach out to our helpline at (+92) 021/051-111-654-321.

SCAN LOGS

Timestamp	Event	Error
2024-10-19 11:02:41	Generating Hashes	OK
2024-10-19 11:02:42	Extracting APK	OK
2024-10-19 11:02:42	Unzipping	OK
2024-10-19 11:02:43	Getting Hardcoded Certificates/Keystores	OK
2024-10-19 11:02:55	Parsing AndroidManifest.xml	OK
2024-10-19 11:02:55	Parsing APK with androguard	OK

2024-10-19 11:02:56	Extracting Manifest Data	OK
2024-10-19 11:02:56	Performing Static Analysis on: JS Mobile (com.JSBL.bank)	OK
2024-10-19 11:02:56	Fetching Details from Play Store: com.JSBL.bank	OK
2024-10-19 11:02:57	Manifest Analysis Started	OK
2024-10-19 11:02:57	Checking for Malware Permissions	OK
2024-10-19 11:02:57	Fetching icon path	OK
2024-10-19 11:02:57	Library Binary Analysis Started	OK
2024-10-19 11:02:57	Reading Code Signing Certificate	OK
2024-10-19 11:03:01	Running APKiD 2.1.5	OK
2024-10-19 11:03:11	Detecting Trackers	OK

2024-10-19 11:03:18	Decompiling APK to Java with jadx	OK
2024-10-19 11:05:04	Converting DEX to Smali	OK
2024-10-19 11:05:04	Code Analysis Started on - java_source	OK
2024-10-19 11:06:10	Android SAST Completed	OK
2024-10-19 11:06:10	Android API Analysis Started	OK
2024-10-19 11:06:53	Android Permission Mapping Started	OK
2024-10-19 11:07:45	Android Permission Mapping Completed	OK
2024-10-19 11:07:53	Finished Code Analysis, Email and URL Extraction	OK
2024-10-19 11:07:53	Extracting String data from APK	OK
2024-10-19 11:07:53	Extracting String data from Code	OK
2024-10-19 11:07:53	Extracting String values and entropies from Code	OK

2024-10-19 11:08:01	Performing Malware check on extracted domains	OK
2024-10-19 11:08:10	Saving to Database	OK

Report Generated by - MobSF v4.0.7

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.