ANDROID STATIC ANALYSIS REPORT

app_icon

BOK Digital (12.0.15)

File Name:	BOK Digital.apk
Package Name:	com.temenos.bok
Scan Date:	Nov. 14, 2024, 8:12 p.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	14	2	3	1

FILE INFORMATION

File Name: BOK Digital.apk
Size: 8.17MB
MD5: 1dc7de976f7e3770c236d88d862bc6eb
SHA1: 36a24d72f2434e0971bc90245279ff154ca53be2
SHA256: 24d60607cd701e8d11ef533375c88aee0c541be75ba3e63257da57132c50aaf8

APP INFORMATION

App Name: BOK Digital
Package Name: com.temenos.bok
Main Activity: com.temenos.bok.ui.login.presenter.LoginActivity
Target SDK: 34
Min SDK: 22
Max SDK:
Android Version Name: 12.0.15

Android Version Code: 35

APP COMPONENTS

Activities: 8
Services: 10
Receivers: 4
Providers: 4
Exported Activities: 0
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: 2020-05-30 09:22:45+00:00
Valid To: 2050-05-30 09:22:45+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x677b38ff269771a57f0ce6abfcb1eeb158ab4c0c
Hash Algorithm: sha256
md5: 19cda3999445f8551e50d6f395a24480
sha1: ebefc9291406a86469ae9397b65d7ab3f84c2d9f
sha256: 86c0afb488ec0771f1ced7261ef161921b435095ad5bd44e1147fff0785c51f6
sha512: a48e65078245202fd6f78cc76af8389bcd3a98ee2c4aeee751ab1f3952eeebe0e4811b02e894a75ee793d29a54704c3edddd193e1871aa4edd1886e6ae69d816
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 0c53fc1efc0bdbfb1ed74aaa5461a6d58931cdfb193993d02a7b68dcfac7b0f5
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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_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_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
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_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.temenos.bok.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
1dc7de976f7e3770c236d88d862bc6eb.apk	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>possible VM check</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 Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check possible VM check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Compiler</td><td>r8</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
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: 1 | WARNING: 3 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.1-5.1.1, [minSdk=22]	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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [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.
3	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.
4	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 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: 8 | INFO: 2 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a8/c.java aa/c.java b1/o.java b4/e.java b5/c.java ba/e.java ba/g.java ba/h.java c1/h.java c1/i.java c1/j.java c8/c.java cc/a.java d/d0.java d/h0.java d1/d.java d8/a.java df/c.java e0/f.java e0/s.java e7/a.java e7/c.java ea/d.java f8/a0.java f8/c0.java f8/e.java f8/e0.java f8/h.java f8/k.java f8/n.java f8/o.java f8/t.java f8/v.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	f8/y.java f8/z.java fe/w.java g0/a.java g2/v.java g3/c.java g3/g.java g3/i.java g7/c.java h0/e.java h1/a.java h7/b.java i/h.java i/p.java i5/c.java i6/c.java i7/g.java i7/j.java i7/l.java i7/n.java i7/p.java i7/r.java i7/s.java i7/t.java i7/u.java i7/w.java i7/x.java j7/d.java j7/j.java j8/o.java j8/s.java k7/x.java ka/b.java l1/c.java l1/f.java l1/p.java l1/x0.java l1/z1.java l4/u.java l8/d.java l8/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				m7/b.java n4/c.java n7/c.java o/k.java o/r1.java o7/b.java ob/a.java p0/d.java p1/u.java p3/e.java p5/b.java q3/b.java q3/c.java q3/d.java q3/g.java q3/h.java q3/i.java q3/k.java q3/l.java q4/b.java q6/c.java r0/f.java r3/h.java r3/i.java r3/n.java r3/r.java r3/v.java s1/d.java t/c.java t3/d.java t3/f.java t3/x.java u/d.java u2/d.java u2/o.java u3/e.java u3/j0.java u3/k0.java u3/n.java u3/v.java u3/y.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				u4/a7.java u4/f7.java u4/y3.java ua/i.java v0/d.java v0/f.java v0/i.java v0/m.java v8/a.java w2/h.java w4/a.java w8/a.java we/l.java x4/a.java x7/d.java x8/b.java x8/c.java xe/d.java y/b.java y1/b.java y3/c.java z0/i.java z0/q0.java z1/c.java z1/f.java z3/a.java z8/b.java
2	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	we/d.java we/g.java we/k.java we/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	e0/s.java u4/g7.java x/f.java y6/a.java yd/a.java yd/b.java zd/a.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') OWASP Top 10: M7: Client Code Quality	e0/f.java g3/c.java g3/h.java g3/i.java h3/g.java h3/m.java o/i.java o/k2.java o/l0.java p6/r.java u4/a7.java u4/c4.java u4/j.java u4/u3.java
5	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	b8/b.java c8/c.java i7/g.java m7/b.java w8/a.java wc/a.java
6	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/tello/digitalonboarding/network/Header.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	MD5 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	u4/g7.java
8	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	ua/i.java
9	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	i7/g.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/temenos/bok/network/request/changeOldPassword/ChangeOldPasswordRequest.java com/temenos/bok/network/request/changePassword/ChangePasswordRequest.java com/temenos/bok/network/request/changeUsername/ChangeUsernameRequest.java com/temenos/bok/network/request/resignUpChangePassword/ReSignUpChangePasswordRequest.java
11	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	e7/c.java sa/d.java v1/b.java
12	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	e0/s.java v8/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
13	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	x/q.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/karumi/dexter/listener/SettingsClickListener.java com/tello/digitalonboarding/ui/digitalOnboarding/presenter/Screen23.java com/temenos/bok/ui/branchLocator/presenter/BranchMap.java com/temenos/bok/ui/qrCode/presenter/QrDetails.java g2/a.java g2/b.java q3/f.java q6/c.java r3/f.java u4/g7.java z8/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/temenos/bok/ui/qrCode/presenter/QrDetails.java e0/s.java
00108	Read the input stream from given URL	network command	u4/b4.java u4/w5.java
00014	Read file into a stream and put it into a JSON object	file	j7/d.java o7/b.java v8/a.java
00022	Open a file from given absolute path of the file	file	e0/s.java e7/c.java j7/d.java ma/e0.java t1/j0.java t1/x.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	c1/h.java c1/i.java d1/d.java i7/g.java j7/d.java l4/u.java m7/a.java n2/a.java n2/i.java o7/b.java org/simpleframework/xml/core/Persister.java org/simpleframework/xml/stream/StreamProvider.java p6/r.java q4/b.java t1/e0.java t1/j0.java u/d.java v1/f.java v8/a.java w8/a.java z1/f.java
00005	Get absolute path of file and put it to JSON object	file	j7/d.java
00089	Connect to a URL and receive input stream from the server	command network	c8/c.java o/k.java ua/b.java
00109	Connect to a URL and get the response code	network command	c8/c.java l3/c.java o/k.java p3/e.java u4/y5.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	b/a.java b5/c.java ua/i.java
00162	Create InetSocketAddress object and connecting to it	socket	we/c.java we/l.java
00163	Create new Socket and connecting to it	socket	we/c.java we/l.java
00147	Get the time of current location	collection location	d/c0.java
00075	Get location of the device	collection location	d/c0.java
00115	Get last known location of the device	collection location	d/c0.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	g2/a.java g2/b.java q6/c.java r3/f.java
00036	Get resource file from res/raw directory	reflection	com/karumi/dexter/listener/SettingsClickListener.java g2/a.java q6/c.java r3/f.java
00189	Get the content of a SMS message	sms	b4/e.java e7/c.java
00188	Get the address of a SMS message	sms	b4/e.java e7/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00200	Query data from the contact list	collection contact	b4/e.java e7/c.java
00201	Query data from the call log	collection calllog	b4/e.java e7/c.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	b4/e.java e7/c.java
00094	Connect to a URL and read data from it	command network	q6/c.java
00096	Connect to a URL and set request method	command network	o/k.java
00183	Get current camera parameters and change the setting.	camera	ba/h.java
00012	Read data and put it into a buffer stream	file	z1/f.java
00123	Save the response to JSON after connecting to the remote server	network command	u4/y5.java
00030	Connect to the remote server through the given URL	network	u4/y5.java
00003	Put the compressed bitmap data into JSON object	camera	x7/d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00126	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	e7/c.java
00125	Check if the given file path exist	file	e7/c.java
00187	Query a URI and check the result	collection sms calllog calendar	e7/c.java
00104	Check if the given path is directory	file	z3/a.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/23757875439/namespaces/firebase:fetch?key=AIzaSyBEnNUuQYIjSDt-CU9yoDDq1oiz9_4GFIU. This is indicated by the response: The response code is 403

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.READ_CONTACTS, android.permission.READ_EXTERNAL_STORAGE, android.permission.WAKE_LOCK, android.permission.CAMERA, android.permission.ACCESS_WIFI_STATE
Other Common Permissions	3/44	com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_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

DOMAIN	STATUS	GEOLOCATION
accounts.google.com	ok	**IP:** 108.177.119.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
mobile.bok.com.pk	ok	**IP:** 103.150.9.32 **Country:** Pakistan **Region:** Islamabad **City:** Islamabad **Latitude:** 33.721481 **Longitude:** 73.043289 **View:** Google Map
ebank.bok.com.pk	ok	**IP:** 103.150.9.36 **Country:** Pakistan **Region:** Islamabad **City:** Islamabad **Latitude:** 33.721481 **Longitude:** 73.043289 **View:** Google Map
maps.google.com	ok	**IP:** 142.250.187.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
journeyapps.com	ok	**IP:** 3.164.85.102 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.187.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
issuetracker.google.com	ok	**IP:** 172.217.169.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
app-measurement.com	ok	**IP:** 142.251.140.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
goo.gl	ok	**IP:** 216.58.212.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.xmlsoap.org	ok	**IP:** 13.107.246.45 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
ipapi.co	ok	**IP:** 104.26.9.44 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebase-settings.crashlytics.com	ok	**IP:** 142.250.187.131 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.googleadservices.com	ok	**IP:** 216.58.214.130 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 216.58.213.98 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
www.google.com	ok	**IP:** 216.58.212.36 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
google.com	ok	**IP:** 142.251.140.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.121.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	r3/p.java

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
OpenTelemetry (OpenCensus, OpenTracing)	Analytics	https://reports.exodus-privacy.eu.org/trackers/412

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "9e98bc0f7c07475cab24cf1a2fef2d7e"
"google_api_key" : "AIzaSyBEnNUuQYIjSDt-CU9yoDDq1oiz9_4GFIU"
"google_crash_reporting_api_key" : "AIzaSyBEnNUuQYIjSDt-CU9yoDDq1oiz9_4GFIU"
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
"password" : "Password"
"username" : "Username"

POSSIBLE SECRETS
sha256/Wec45nQiFwKvHtuHxSAMGkt19k+uPSw9JlEkxhvYPHk=
470fa2b4ae81cd56ecbcda9735803434cec591fa

PLAYSTORE INFORMATION

Title: BOK Digital

Score: 2.2962964 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Finance **Play Store URL:** com.temenos.bok

Developer Details: Bank of Khyber, Bank+of+Khyber, None, https://www.bok.com.pk/, complaints@bok.com.pk,

Release Date: Jun 1, 2020 **Privacy Policy:** Privacy link

Description:

Embark on a revolutionary banking journey with the Bank of Khyber (BoK - Digital) Android app – your gateway to seamless financial management. Crafted exclusively for BOK customers, our app redefines convenience and sophistication, bringing banking to your fingertips like never before. Unlock the Potential: 1. Effortless Registration: Joining the BOK family is a breeze. Existing customers can swiftly register or sign up, getting them started on their banking voyage in moments. 2. Streamlined Login Experience: Say goodbye to cumbersome login processes. With our app, your first-time login is seamlessly integrated with device registration, ensuring a hassle-free initiation. 3. Robust Security Measures: Your security is paramount. Utilizing Two-Factor Authentication via OTP, we provide peace of mind, safeguarding your transactions and data with industry-leading protocols. 4. Instant Balance Checks: Stay informed with a glance. Effortlessly monitor your account balances anytime, anywhere, putting financial insights at your fingertips. 5. Comprehensive Account Insights: Dive deeper into your finances. Access detailed statements and mini statements with ease, empowering you with unparalleled transparency. 6. Effortless Funds Transfer: Managing your funds has never been simpler. Enjoy hassle-free transfers within BOK accounts, ensuring swift and secure transactions. 7. Seamless Raast Payments: Embrace the future of payments. Our app seamlessly integrates Raast Payments, facilitating instant and efficient transactions for your convenience. 8. Convenient IBFT Services: Bridge the gap effortlessly. Conduct IBFT transfers to other banks seamlessly, expanding your financial reach with just a few taps. 9. Simplified Utility Payments: Bid farewell to bill payment woes. Our UBPS feature streamlines utility bill payments, ensuring a frictionless experience every time. 10. Mobile Top-Ups on the Go: Stay connected effortlessly. Enjoy the convenience of mobile top-ups directly through our app, keeping you connected with loved ones effortlessly. 11. Effortless Beneficiary Management: Manage beneficiaries with ease. Create, review, and update beneficiary information conveniently, putting you in control of your transactions. 12. Hassle-Free Postpaid Bill Settlements: Say goodbye to overdue bills. Our app simplifies postpaid bill payments, ensuring timely settlements without the stress. 13. Limit Management: Take charge of your finances with ease. Manage your transaction limits effortlessly, customizing them to suit your financial needs and preferences. 13. Card Management Empowerment: Your cards, your control. With our card management system, take charge by changing PINs and managing card activation/deactivation seamlessly. 14. QR Code Generation: Seamlessly generate QR codes for instant transactions. Whether for payments or identification, our app puts the power of QR technology in your hands. 15. Payment through QR Code: Experience unparalleled convenience with QR code payments. Simply scan and pay, revolutionizing the way you transact securely and swiftly. 16. Login through

Fingerprint: Access your account securely and swiftly with fingerprint authentication, ensuring a seamless login experience every time 17. Manage Multiple Accounts under One Login: Simplify your financial management. Access and manage multiple accounts under a single login, streamlining your banking experience. Unleash the Power of Banking: Experience banking reimagined with the Bank of Khyber Android app. Designed for the discerning Android user, our app combines cutting-edge technology with intuitive design, setting new standards for mobile banking excellence. Download now and embark on a journey where convenience meets sophistication. Elevate your banking experience – because you deserve nothing less. For queries and complaints, please contact us at +92-91-111-265-265 or email us at complaints@bok.com.pk

SCAN LOGS

Timestamp	Event	Error
2024-11-14 20:12:30	Generating Hashes	OK
2024-11-14 20:12:30	Extracting APK	OK
2024-11-14 20:12:30	Unzipping	OK
2024-11-14 20:12:30	Getting Hardcoded Certificates/Keystores	OK
2024-11-14 20:12:30	Parsing APK with androguard	OK
2024-11-14 20:12:33	Parsing AndroidManifest.xml	OK
2024-11-14 20:12:33	Extracting Manifest Data	OK

2024-11-14 20:12:33	Performing Static Analysis on: BOK Digital (com.temenos.bok)	OK
2024-11-14 20:12:33	Fetching Details from Play Store: com.temenos.bok	OK
2024-11-14 20:12:35	Manifest Analysis Started	OK
2024-11-14 20:12:35	Checking for Malware Permissions	OK
2024-11-14 20:12:35	Fetching icon path	OK
2024-11-14 20:12:35	Library Binary Analysis Started	OK
2024-11-14 20:12:35	Reading Code Signing Certificate	OK
2024-11-14 20:12:36	Running APKiD 2.1.5	OK
2024-11-14 20:12:39	Detecting Trackers	OK
2024-11-14 20:12:40	Decompiling APK to Java with JADX	OK
2024-11-14 20:12:52	Converting DEX to Smali	OK

2024-11-14 20:12:52	Code Analysis Started on - java_source	OK
2024-11-14 20:13:00	Android SAST Completed	OK
2024-11-14 20:13:00	Android API Analysis Started	OK
2024-11-14 20:13:08	Android API Analysis Completed	OK
2024-11-14 20:13:09	Android Permission Mapping Started	OK
2024-11-14 20:13:18	Android Permission Mapping Completed	OK
2024-11-14 20:13:19	Email and URL Extraction Completed	OK
2024-11-14 20:13:19	Android Behaviour Analysis Started	OK
2024-11-14 20:13:28	Android Behaviour Analysis Completed	OK
2024-11-14 20:13:28	Extracting String data from APK	OK
2024-11-14 20:13:28	Extracting String data from Code	OK

2024-11-14 20:13:28	Extracting String values and entropies from Code	OK
2024-11-14 20:13:30	Performing Malware check on extracted domains	OK
2024-11-14 20:13:41	Saving to Database	OK

Report Generated by - MobSF v4.1.9

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.