



ANDROID STATIC ANALYSIS REPORT



 Gov.br (3.4.1)

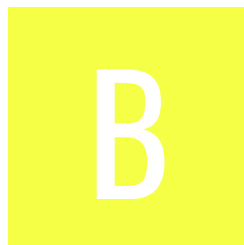
File Name: govbr.apk

Package Name: br.gov.meugovbr

Scan Date: June 20, 2023, 8:58 p.m.






App Security Score: 55/100 (MEDIUM RISK)

Grade:



Trackers Detection: 2/428

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
1	13	2	2	2

FILE INFORMATION

File Name: govbr.apk

Size: 15.66MB

MD5: 764898b0cddb4aba5af53d9f6d593986

SHA1: d4a0d25e1d0516cb8699986eed062fb3d3b179f1

SHA256: 81acab48775ba8fea248046ecd8e3bb3224f2dad774ae52af976a6a66bc6afae

APP INFORMATION

App Name: Gov.br

Package Name: br.gov.meugovbr

Main Activity: br.gov.meugovbr.MainActivity

Target SDK: 33

Min SDK: 23

Max SDK:

Android Version Name: 3.4.1

Android Version Code: 130

APP COMPONENTS

Activities: 10

Services: 8

Receivers: 4

Providers: 5

Exported Activities: 0

Exported Services: 0

Exported Receivers: 2

Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed

v1 signature: True

v2 signature: True

v3 signature: True

Found 1 unique certificates

Subject: C=BR, ST=Bahia, L=Salvador, O=Serpro, OU=DGGD3, CN=Danilo Costa Viana

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2020-04-02 22:27:26+00:00

Valid To: 2070-03-21 22:27:26+00:00

Issuer: C=BR, ST=Bahia, L=Salvador, O=Serpro, OU=DGGD3, CN=Danilo Costa Viana

Serial Number: 0x430a7f1d

Hash Algorithm: sha256

md5: d4e8408d9bf7cd89796fe2be90b59b04

sha1: 67615ec97d20a656ab51f279418271bce4a17520

sha256: e133067fc50bda439c1fc61aa80cd5f238dc65b34d8d303bff4a33ae2f4705ab

sha512: 14c86f9e8c564722fd2684439e556a1b9d6c0d1f0577dbe44c5d5160e3e35ada3d2e0fef5dcca09cba47c69f7567f6bcab0afa07a731c3cecf2f0bfce502a9f7

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 17163d0564b1854096f4eb19e603b21005ab4fe7d5837d202350a9d541a13431

☰ APPLICATION PERMISSIONS

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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.POST_NOTIFICATIONS	unknown	Unknown permission	Unknown permission from android reference
android.permission.USE_BIOMETRIC	normal		Allows an app to use device supported biometric modalities.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
br.gov.meugovbr.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.hardware.camera.autofocus	unknown	Unknown permission	Unknown permission from android reference
android.permission.HIGH_SAMPLING_RATE_SENSORS	normal	Access higher sampling rate sensor data	Allows an app to access sensor data with a sampling rate greater than 200 Hz.
android.permission.RECORD_VIDEO	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
------	---------

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check Build.TAGS check SIM operator check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	dx

ACTIVITY	INTENT
br.gov.meugovbr.MainActivity	Schemes: meugovbr://, https://, Hosts: logged, logout, senha, login, login-qr-code, device-authorization, meugovhom.page.link, meugovbr.page.link,

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: 0 | WARNING: 3 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version [minSdk=23]	warning	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. Support an Android version > 8, API 26 to receive reasonable security updates.
2	Broadcast Receiver (io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingReceiver) 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.
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.

</> CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a2/a.java b1/a.java b6/j.java b8/a.java c0/b.java c0/b0.java c0/d0.java c0/g.java c0/j0.java c0/k.java c0/z.java c1/h.java c6/e.java c6/l.java c9/a.java com/identity/face/FaceActivity.java com/identity/face/FaceBaseProcessor.java com/identity/face/FaceIntroActivity.java com/identity/face/FaceProcessor.java com/identity/face/FaceRegion.java com/identity/face/FileUtils.java com/identity/face/GCTestActivity.java com/identity/face/IdentyFaceSdk.java com/identity/face/MainActivity.java com/identity/face/VerifyFaceActivity.java com/identity/face/b/getQt.java com/identity/face/b/getSf.java com/identity/face/camera/b/getQt.java com/identity/face/camera/cameracontrolle r/AS.java com/identity/face/camera/cameracontrolle r/values.java com/identity/face/d/isC1.java com/identity/face/d/values.java com/identity/face/isC1.java com/identity/face/xlog/b/getQt.java com/journeyapps/barcodescanner/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				<div>com/journeyapps/barcodescanner/b.java</div> <div>d/f.java</div> <div>d/h.java</div> <div>d/j.java</div> <div>d0/b.java</div> <div>e0/c.java</div> <div>ed/b.java</div> <div>f0/c.java</div> <div>f0/d.java</div> <div>f0/i.java</div> <div>f0/k.java</div> <div>f1/b.java</div> <div>f1/c.java</div> <div>f8/d.java</div> <div>f9/n.java</div> <div>g1/b.java</div> <div>g5/g.java</div> <div>h/g.java</div> <div>h8/b.java</div> <div>i/c.java</div> <div>i2/a.java</div> <div>i2/d.java</div> <div>i4/e.java</div> <div>io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingBackgroundService.java</div> <div>io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingReceiver.java</div> <div>io/flutter/plugins/firebase/messaging/a.java</div> <div>io/flutter/plugins/firebase/messaging/e.java</div> <div>io/flutter/plugins/firebase/messaging/z.java</div> <div>io/flutter/plugins/imagepicker/a.java</div> <div>io/flutter/plugins/imagepicker/n.java</div> <div>io/flutter/plugins/pathprovider/a.java</div> <div>io/flutter/plugins/url_launcher/a.java</div> <div>io/flutter/plugins/url_launcher/b.java</div>

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	j/a1.java j/a.java j/d0.java j/k0.java j/m0.java j/n0.java j/q0.java j/r0.java j/w.java j/z.java j/z0.java j0/a.java j0/b.java j1/f.java l3/a.java m2/b.java m2/g.java m2/q.java m2/s.java m2/v.java m3/a.java m7/a.java m7/e.java m9/a.java n0/a.java n1/a.java n1/n.java n1/o.java n1/p.java n2/e.java n2/h.java n2/k.java n2/t.java n2/x.java n7/h.java nd/c.java o5/k.java o5/r.java o7/l.java p/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				p/h.java p/t.java p2/a0.java p2/b0.java p2/o0.java p2/t0.java p3/i.java p4/g.java p4/o.java p7/a.java p7/c.java p7/g.java p7/h.java p7/l.java p7/n.java p7/q.java q/a.java q0/b.java r2/a.java r2/q0.java r2/r0.java r2/w0.java r2/x.java r2/z0.java r5/a.java r6/e.java r6/g.java s/c.java s/d.java s/h.java s0/a.java s4/f.java s6/a.java t/d.java t/f.java t/g.java t/h.java t/k.java t/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				t0/d.java t0/e.java u/a.java u/e.java u2/a.java u5/c.java v2/g.java v2/l.java v2/m.java v4/m.java x1/f.java x5/c.java x5/c0.java x5/c1.java x5/d.java x5/e0.java x5/g.java x5/g0.java x5/j0.java x5/k.java x5/n.java x5/n0.java x5/p0.java x5/q0.java x5/r0.java x5/u0.java x5/v0.java x5/z0.java y/l.java y0/c.java z2/b.java z3/a.java z3/b.java z3/c.java
2	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/identity/face/FaceProcessor.java com/identity/face/IdentyFaceSdk.java com/identity/face/users/IdentyUserManag er.java f1/a.java x4/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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/identity/face/IdentyFaceSdk.java com/identity/face/LManager.java com/identity/face/LicenseValidator.java o5/k.java t5/b.java x5/c0.java
4	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	j1/a.java s7/a.java
5	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/identity/face/FileUtils.java io/flutter/plugins/pathprovider/a.java k9/g.java l9/b.java q/a.java q/b.java
6	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	e2/m0.java e2/p0.java e2/t0.java z0/a.java
7	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	b6/q.java fa/a.java fa/b.java ga/a.java
8	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	com/identity/face/LManager.java n7/h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	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/journeyapps/barcodescanner/b.java j0/a.java j3/b.java t5/c.java
10	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	io/flutter/plugin/editing/b.java io/flutter/plugin/platform/c.java
11	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	p3/v.java v4/h.java
12	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	md/e.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application implement asymmetric key generation.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['location', 'network connectivity', 'camera'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_CKM.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Asymmetric Key Generation	The application generate asymmetric cryptographic keys not in accordance with FCS_CKM.1.1(1) using key generation algorithm RSA schemes and cryptographic key sizes of 1024-bit or lower.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
12	FCS_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption in accordance with a specified cryptographic algorithm AES-CBC (as defined in NIST SP 800-38A) mode or AES-GCM (as defined in NIST SP 800-38D) and cryptographic key sizes 256-bit/128-bit.
13	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
14	FCS_COP.1.1(3)	Selection-Based Security Functional Requirements	Cryptographic Operation - Signing	The application perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm RSA schemes using cryptographic key sizes of 2048-bit or greater.
15	FCS_COP.1.1(4)	Selection-Based Security Functional Requirements	Cryptographic Operation - Keyed-Hash Message Authentication	The application perform keyed-hash message authentication with cryptographic algorithm ['HMAC-SHA-256'] .
16	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
17	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
18	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
19	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.
20	FPT_TUD_EXT.2.1	Selection-Based Security Functional Requirements	Integrity for Installation and Update	The application shall be distributed using the format of the platform-supported package manager.
21	FCS_CKM.1.1(2)	Optional Security Functional Requirements	Cryptographic Symmetric Key Generation	The application shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes 128 bit or 256 bit.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
journeyapps.com	ok	IP: 18.161.200.38 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map

DOMAIN	STATUS	GEOLOCATION
xml.apache.org	ok	IP: 151.101.2.132 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
firebase.google.com	ok	IP: 142.251.135.46 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
github.com	ok	IP: 20.201.28.151 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
appmeugov.firebaseio.com	ok	IP: 34.120.160.131 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map

DOMAIN	STATUS	GEOLOCATION
liveness.serpro.gov.br	ok	IP: 161.148.122.4 Country: Brazil Region: Distrito Federal City: Brasilia Latitude: -15.779720 Longitude: -47.929722 View: Google Map
developer.android.com	ok	IP: 142.250.78.206 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
firebase-settings.crashlytics.com	ok	IP: 142.250.79.163 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
api.ipify.org	ok	IP: 173.231.16.76 Country: United States of America Region: Utah City: Ogden Latitude: 41.276379 Longitude: -111.987442 View: Google Map

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	IP: 142.250.79.46 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.
pagead2.googlesyndication.com	ok	IP: 142.250.79.34 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
plus.google.com	ok	IP: 142.251.129.78 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.

DOMAIN	STATUS	GEOLOCATION
licensemgr.identity.io	ok	IP: 34.225.240.69 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://appmeugov.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	n2/s.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

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://appmeugov.firebaseio.com"
"google_api_key" : "AlzaSyCbclvH6-pH9PjsWyWmVkqHUTAGiDzalmk"
"google_crash_reporting_api_key" : "AlzaSyCbclvH6-pH9PjsWyWmVkqHUTAGiDzalmk"
"library_xingandroidembedded_author" : "JourneyApps"
"library_xingandroidembedded_authorWebsite" : "https://journeyapps.com/"
"nec_clientSecret" : "e2b70ab4-824e-48a6-a3f5-69e5e4896186"

PLAYSTORE INFORMATION

Title: gov.br

Score: 4.6884356 **Installs:** 50,000,000+ **Price:** 0 **Android Version Support:** Category: Tools **Play Store URL:** [br.gov.meugovbr](https://play.google.com/store/apps/details?id=br.gov.meugovbr)

Developer Details: Serviços e Informações do Brasil, 5829287075355252046, None, None, atendimentogovbr@economia.gov.br,

Release Date: Aug 26, 2020 **Privacy Policy:** [Privacy link](#)

Description:

Now yes! We have a new look! And with news! The "gov.br" app (formerly My gov.br) is renewed for you to have a more simplified experience: - For starters, you can access the app without doing facial recognition and if you need to create your gov.br account, we'll do it through the app. - You can access any government service that has the "Enter with gov.br" button without needing a password, using only your cell phone's biometrics. Will you forget the password?! - And more, in addition to being able to consult your data and digital documents, you can share them with your contacts to make life easier. You can also see your login history on gov.br sites and have more transparency to understand how they are using your data. - And to make your account more secure, you can level it up to silver or gold! All of this available in the new app, keeping what was already useful: digital proof of life, receiving notifications to sign electronic documents and much more!

Report Generated by - MobSF v3.6.7 Beta

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.

© 2023 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).