Test security and privacy of your mobile application (iOS & Android), detect OWASP Mobile Top 10 and other weaknesses.

Summary of Mobile Application Security Test

APP NAME	APP ID	APP VERSION
Covid19Verify	lv.verification.dgc	4

DEVICE TYPE	TEST STARTED	TEST FINISHED
iOS	May 9th 2022, 21:20	May 9th 2022, 21:26

Mobile App Permissions and Privacy	OWASP Mobile Top 10 Security Test	Mobile App External Communications	Software Composition Analysis
1 PERMISSION	1 MAJOR RISK FOUND	NOT FOUND	19 COMPONENTS FOUND

Malware test: no malicious code or behavioral patterns detected in the mobile app.

Mobile Application Permissions and Privacy Test

Mobile Application Functionality

The mobile application requests access to the following functionality that may endanger user's privacy under certain circumstances:

Camera

The mobile application can use phone’s camera for taking pictures or videos.

Mobile Application Permissions

The mobile application requests the following permissions that may endanger user's privacy under certain circumstances:

NSCameraUsageDescription dangerous

Access Camera.

OWASP Mobile Top 10 Security Test

Your application is not compiled for iOS simulator, dynamic testing will be skipped and many vulnerabilities may remain undetected. We suggest to recompile your mobile app and try again.

The automated audit revealed the following security flaws and weaknesses that may impact the application:

HIGH RISK	MEDIUM RISK	LOW RISK	WARNINGS
0	0	0	2

Zero false-positive SLA and advanced manual testing of application is only available in ImmuniWeb® MobileSuite.

MISSING ANTI-EMULATION [SAST]

WARNING

Description:

The mobile application does not use any anti-emulation or anti-debugger techniques (e.g. detecting rooted devices or checking if contacts are authentic).
This can significantly facilitate application debugging and reverse-engineering processes.

DISABLED APP TRANSPORT SECURITY (ATS) [M3] [CWE-319] [SAST]

WARNING

Description:

ATS should be configured according to best practices by Apple and only be deactivated under certain circumstances.

Details:

There is **'NSAllowsArbitraryLoads'** found in file 'ios/Payload/ios.app/Info.plist':

Software Composition Analysis Test

The mobile application uses the following external and native libraries:

External

- @rpath/Capacitor.framework/Capacitor
- @rpath/CapacitorApp.framework/CapacitorApp
- @rpath/CapacitorCommunityHttp.framework/CapacitorCommunityHttp
- @rpath/CapacitorCommunitySqlite.framework/CapacitorCommunitySqlite
- @rpath/CapacitorDevice.framework/CapacitorDevice

- @rpath/CapacitorDialog.framework/CapacitorDialog
- @rpath/CapacitorFilesystem.framework/CapacitorFilesystem
- @rpath/CapacitorHaptics.framework/CapacitorHaptics
- @rpath/CapacitorNetwork.framework/CapacitorNetwork
- @rpath/CapacitorSecureStoragePlugin.framework/CapacitorSecureStoragePlugin
- @rpath/CapacitorSplashScreen.framework/CapacitorSplashScreen
- @rpath/CapacitorStorage.framework/CapacitorStorage
- @rpath/Cordova.framework/Cordova
- @rpath/DigitalGreenCertificateBarcodeScannerFork.framework/DigitalGreenCertificateBarcodeScannerFo
- @rpath/DigitalGreenCertificateCapacitorAppUpdatePlugin.framework/DigitalGreenCertificateCapacitorApp
- @rpath/Reachability.framework/Reachability
- @rpath/SQLCipher.framework/SQLCipher
- @rpath/SwiftKeychainWrapper.framework/SwiftKeychainWrapper
- @rpath/ZIPFoundation.framework/ZIPFoundation