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
GreenCheck	at.itsv.mobile.cochap	251
DEVICE TYPE	**TEST STARTED**	**TEST FINISHED**
iOS	May 9th 2022, 21:37	May 9th 2022, 21:48

Mobile App Permissions and Privacy	OWASP Mobile Top 10 Security Test	Mobile App External Communications	Software Composition Analysis
3 PERMISSIONS	**1 MAJOR RISK FOUND**	**NOT FOUND**	**NO 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:

Accelerometer

The mobile application can use device’s accelerometers.

Camera

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

Microphone

The mobile application can record audio using phone’s microphone.

Location

The mobile application has an access to user geographical location.

Mobile Application Permissions

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

NSCameraUsageDescription dangerous

Access Camera.

NSMicrophoneUsageDescription dangerous

Access microphone.

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	WARNING
0	0	0	1

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.

Software Composition Analysis Test

The mobile application seems not to use any external or native libraries.

External	Native
None	None