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
N/A	edu.mit.privatekit	null
DEVICE TYPE	**TEST STARTED**	**TEST FINISHED**
Android	March 19th 2020, 14:57	March 19th 2020, 15:20

DAST was not performed because the uploaded Android application is not compiled for x86 Emulator.

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

OWASP Mobile Top 10

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

WARNINGS	LOW RISK	MEDIUM RISK	HIGH RISK
2	0	0	0

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.

Reference:

- https://github.com/strazzere/anti-emulator

NETWORK SECURITY CONFIGURATION IS NOT PRESENT [SAST]

WARNING

Description:
The mobile application does not use Network Security Configuration to define which certificates and Certificate Authorities (CA) can be used for different environments (e.g. Development, Test and Production). The Network Security Configuration on Android feature lets application developers customize their network security settings in a safe, declarative configuration file without modifying the application code.

Reference:

- https://developer.android.com/training/articles/security-config.html