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
Coronapas	dk.sum.ssicpas	269
DEVICE TYPE	**TEST STARTED**	**TEST FINISHED**
iOS	May 9th 2022, 18:54	May 9th 2022, 19:18

Mobile App Permissions and Privacy

2 PERMISSIONS

OWASP Mobile Top 10 Security Test

1 MAJOR RISK FOUND

Mobile App External Communications

RISKS FOUND

Software Composition Analysis

NO COMPONENTS FOUND

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:

Location

The mobile application has an access to user geographical location.

Contacts

The mobile application can read or write to user's contacts.

Media

The mobile application has an access to mobile phone’s media (e.g. music or photo) in read and/or write mode.

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.

Accelerometer

The mobile application can use device’s accelerometers.

Face ID

The mobile application can use Apple’s Face ID.

Mobile Application Permissions

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

NSCameraUsageDescription dangerous

Access Camera.

NSFaceIDUsageDescription normal

Access the ability to authenticate with Face ID.

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	1	1

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

HARDCODED DATA [M2] [CWE-200] [SAST]

LOW

Description:

The mobile application contains debugging or other technical information that may be extracted and used by an attacker to facilitate further attacks.

http:// with value http://purl.org/dc/elements/1.1/ in following files:

- **ios/Payload/ios.app/Frameworks/libSkiaSharp.framework/libSkiaSharp:**

```
[line 37088: xmlns:dc="http://purl.org/dc/elements/1.1/"]
```

http:// with value http://www.aiim.org/pdfa/ns/id/ in following files:

- **ios/Payload/ios.app/Frameworks/libSkiaSharp.framework/libSkiaSharp:**

```
[line 37091: xmlns:pdfaid="http://www.aiim.org/pdfa/ns/id/">]
```

CVSSv3 Base Score:

3.3 (AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

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.

External Communications and Outgoing Traffic

Mobile Application Endpoints

Static mobile application security test revealed the following remote hosts where the mobile application may send or receive data:

Hostname	IP:Port	SSL Encryption	Websec Server Security	Domain Domain Security
purl.org:80	207.241.239.242:80	N	Not Tested Yet	Not Tested Yet
www.aiim.org:80	199.60.103.225:80	N	C	Not Tested Yet

Software Composition Analysis Test

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

External	Native
None	None