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
Grüner Pass	at.gv.brz.wallet	79
DEVICE TYPE	**TEST STARTED**	**TEST FINISHED**
iOS	May 9th 2022, 21:29	May 9th 2022, 21:35

Mobile App Permissions and Privacy

2 PERMISSIONS

OWASP Mobile Top 10 Security Test

1 MAJOR RISK FOUND

Mobile App External Communications

NO ISSUES FOUND

Software Composition Analysis

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:

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	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.

https:// with value https://id.uvci.eu/DGC.combined-schema.json in following files:

- **ios/Payload/ios.app/ios:**

```
[line 8577: "$id": "https://id.uvci.eu/DGC.combined-schema.json",]
```

https:// with value https://semver.org/ in following files:

- **ios/Payload/ios.app/ios:**

```
[line 8590: "description": "Version of the schema, according to Semantic
versioning (ISO, https://semver.org/ version 2.0.0 or newer)",]
```

https:// with value https://ec.europa.eu/health/sites/health/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf in following files:

- **ios/Payload/ios.app/ios:**

```
[line 8702: "description": "Certificate Identifier, format as per UVCI:
Annex 2 in
https://ec.europa.eu/health/sites/health/files/ehealth/docs/vaccination-
proof_interoperability-guidelines_en.pdf",]
```

http:// with value http://www.sitemaps.org/schemas/sitemap/0.9 in following files:

- **ios/Payload/ios.app/Impressum/sitemap.xml:**

```
[line 2: <sitemapindex xmlns="http://www.sitemaps.org/schemas/sitemap/0.9">]
```

- **ios/Payload/ios.app/Impressum/de/sitemap.xml:**

```
[line 2: <urlset xmlns="http://www.sitemaps.org/schemas/sitemap/0.9"]
```

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
www.sitemaps.org:80	Not Resolved:80	Not Tested Yet	Not Tested Yet	Not Tested Yet
id.uvci.eu:443	Not Resolved:443	Not Tested Yet	Not Tested Yet	Not Tested Yet
semver.org:443	Not Resolved:443	Not Tested Yet	Not Tested Yet	Not Tested Yet
ec.europa.eu:443	147.67.34.30:443	A+	Not Tested Yet	Not Tested Yet

Software Composition Analysis Test

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

External	Native
None	None