

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

Covid Check

### APP ID

ch.admin.bag.covidcertificate....

### APP VERSION

220411.1820.99268

### DEVICE TYPE

iOS

### TEST STARTED

May 9th 2022, 21:51

### TEST FINISHED

May 9th 2022, 21:57



Mobile App  
Permissions and Privacy

3 PERMISSIONS



OWASP Mobile  
Top 10 Security Test

1 MAJOR RISK FOUND



Mobile App External  
Communications

RISKS 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

0

MEDIUM RISK

0

LOW RISK

1

WARNING

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://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/it/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

## External Communications and External 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
<a href="http://www.sitemaps.org:80">www.sitemaps.org:80</a>	20.40.202.27:80	N	C+	Not Tested Yet

## Software Composition Analysis Test

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

**External**  
None

**Native**  
None