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
iGoat-Swift	OWASP.iGoat-Swift	1
DEVICE TYPE	**TEST STARTED**	**TEST FINISHED**
iOS	February 2nd 2022, 17:02	February 2nd 2022, 17:07

Mobile App Permissions and Privacy	OWASP Mobile Top 10 Security Test	Mobile App External Communications	Software Composition Analysis
1 PERMISSION	1 MAJOR RISK FOUND	RISKS 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:

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:

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	WARNINGS
0	0	1	2

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://realm.io/pricing/. in following files:

- **ios/Payload/ios.app/Frameworks/Realm.framework/LICENSE:**

```
[line 168: http://realm.io/pricing/.]
```

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.

DISABLED APP TRANSPORT SECURITY (ATS) [M3] [CWE-319] [SAST]

WARNING

Description:

ATS should be configured according to best practices by Apple and only be deactivated under certain circumstances.

Details:

There is **'NSAllowsArbitraryLoads'** found in file 'ios/Payload/ios.app/Info.plist':

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
realm.io:80	13.225.214.66:80	Not Tested Yet	B	Not Tested Yet

Software Composition Analysis Test

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

External
None

Native
None