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
DVIA-v2	com.highaltitudehacks.DVIAs…	1
DEVICE TYPE	**TEST STARTED**	**TEST FINISHED**
iOS	February 2nd 2022, 16:59	February 2nd 2022, 17:07

Mobile App Permissions and Privacy	OWASP Mobile Top 10 Security Test	Mobile App External Communications	Software Composition Analysis
2 PERMISSIONS	2 MAJOR RISKS FOUND	NOT FOUND	5 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:

Location

The mobile application has an access to user geographical location.

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.

NSLocationWhenInUseUsageDescription dangerous

Access location information when app is in the foreground.

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
1	0	0	2

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

POSSIBLE MAN-IN-THE-MIDDLE ATTACK [M3] [CWE-297] [SAST]

HIGH

Description:

The mobile application may be vulnerable to a MITM (Man-in-the-Middle) attack.
When a mobile app connects to the backend (e.g. API or web service), missing or improperly implemented hostname verification exposes its users to MITM attacks under certain conditions (e.g. when the attacker can intercept traffic by being in the same wireless network). In case of a successful exploitation, the attacker will be able to intercept and manipulate HTTPS traffic, steal and falsify sensitive data sent or received by the app.

Details:

There is **'canAuthenticateAgainstProtectionSpace'** found in file '1/NSURLConnectionDelegate-Protocol.h':

```
[line 15: - (void)connection:(NSURLConnection *)arg1 didReceiveAuthenticationChallenge:
(NSURLAuthenticationChallenge *)arg2;]
[line 16: - (_Bool)connection:(NSURLConnection *)arg1
canAuthenticateAgainstProtectionSpace:(NSURLProtectionSpace *)arg2;]
[line 17: - (void)connection:(NSURLConnection *)arg1
willSendRequestForAuthenticationChallenge:(NSURLAuthenticationChallenge *)arg2;]
```

CVSSv3 Base Score:

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

Reference:

- https://developer.apple.com/library/content/documentation/NetworkingInternetWeb/Conceptual/NetworkingOverview/SecureNetworking/SecureNetworking.html

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':

Software Composition Analysis Test

The mobile application uses the following external and native libraries:

External

- @rpath/Bolts.framework/Bolts
- @rpath/Flurry_iOS_SDK.framework/Flurry_iOS_SDK
- @rpath/Parse.framework/Parse
- @rpath/Realm.framework/Realm
- @rpath/RealmSwift.framework/RealmSwift

iOS Native

None