

CONSUMER MOBILE APP · IOS & ANDROID

Four high-risk flaws across an iOS and Android app

Mobile app penetration test · OWASP MSTG · iOS & Android

11

FINDINGS

4

HIGH-SEVERITY

**iOS +
Android**

BOTH PLATFORMS

THE CHALLENGE

A mobile app published on both iOS and Android needed a manual test of the client, its backend APIs, and supporting services, with static and dynamic analysis across both platforms.

01

Scope

The apps, backend APIs, test accounts and rules of engagement agreed in writing, with a fixed price before any work began.

02

Static and dynamic analysis

Senior testers decompiled and instrumented both builds and exercised them live to the OWASP MSTG: storage, transport, cryptography, platform config and the backend.

03

Escalate

Anything high-risk is escalated to the client's team as soon as it is confirmed, not held back for the final report.

04

Report and retest

A report mapped to the MSTG with reproduction steps, sequenced by severity, and a free retest of every fix.

WHAT WE FOUND

HIGH

The Android build could install on Android 7.0 (minSdk 24), an unsupported version exposed to known WebView code-execution flaws such as CVE-2017-0780.

HIGH

Cleartext (unencrypted) network traffic was permitted, and a SQL injection flaw let crafted input reach a backend database query.

HIGH

Weak cryptography: AES in CBC mode with PKCS5 / PKCS7 padding, open to a padding-oracle attack that can decrypt or forge data without the key.

THE OUTCOME

Delivered a report mapped to the OWASP Mobile Security Testing Guide covering both platforms, sequenced by severity, with a free retest of every fix once the team had remediated.

A SIMILAR ENGAGEMENT TODAY

Mobile app penetration test, Medium

A feature-rich app on both platforms with several roles and a backend API. Fixed in writing before work begins, free retest included.

FROM

\$8,500

PUBLISHED PRICE · USD

Get a fixed-price quote

Scope in one short form. Proposal within one business day.

invadel.com/scope

info@invadel.com · +1 (929) 591-9013