Mobile Penetration Testing Methodology

Our mobile pen testing methodology (which includes manual + automated) covers all client side mobile application testing and binary analysis including relevant OWASP Mobile Top 10 categories. Below is the methodology that is used for a comprehensive security review of mobile applications: -

Application Enumeration and Profiling

During this phase, testers map the features of the application and enlist the types of data it processes to identify likely attack surfaces and sensitive flows (authentication, data storage, APIs, third-party integrations). This contextual profiling guides targeted test cases, helps prioritise high-risk areas, and ensures critical entry points aren't missed or misclassified.

Security Control and Test Cases

1. **Data Storage Security** – This category focuses on identifying vulnerabilities in how an application handles data storage. It includes checking for sensitive information like credentials, session, hard-coded secrets, API keys etc. in local storage, caching of data, and use of weak encryption methods, clipboard memory, and persistence of data after logout or application uninstallation etc.
2. **Network Communication/Device & Platform Security** – This category focuses on the security of data transmission and the overall device/platform interaction. It includes checking for insecure transmission of data, certificate validation, possibility of MiTM attacks, exposure of API endpoints, and measures for root/jailbreak detection mechanisms etc.
3. **Permissions & App Logic** – This category focuses on assessing how permissions are requested and utilized, ensuring that the app does not overreach. It includes checks like reverse engineering to identify back-doors, debugging tools enabled, manifest permissions to identify unnecessary/excessive access, and code obfuscation etc.
4. **Third-Party Dependencies** – This category focuses on identifying vulnerabilities in the libraries being used, particularly if outdated versions are implemented and ensuring that excessive permissions are granted to third party components etc.
5. **Unauthorized Data Collection** – This category focuses on verification of the collection of Personally Identifiable Information (PII), such as names, email addresses, or geo-location data, without user consent to identify compliance issues if any.

The list provided is not limited to but represents core test cases, but the high level methodology varies based on the logic/business use case of the application being tested.

contactus@blueinfy.net

Actionable Report with Zero False Positives

A key deliverable of the assessment is a highly actionable, well-structured report designed to drive immediate remediation. The report is curated to maintain zero false positives and includes the following critical components: -

- Executive Summary
- Description of Discovered Vulnerabilities
- Risk Rating (curated after business impact assessment and industry security standards like CVSS/CWE/CVE)
- Evidence of Vulnerabilities (screenshots, HTTP traffic, filepath, vulnerable parameter, exploit vector, tool results, reproduction steps etc.)
- Exploit Evidence of Vulnerabilities (if required)
- Mitigation Strategies and Defence Approaches (catered to help Developers)
- Report Readout and Guidance

Tools

Blueinfy uses its own tools along with open source tools and products during the assessment process. Blueinfy has its own tools and utilities for performing manual penetration testing. Some of these tools are available at https://www.blueinfy.com/tools.html