Mobile app security, in concrete terms.

Mobile app security is the practice of keeping iOS and Android applications, and the backend APIs behind them, from being abused by attackers. A mobile app is different from a web app in one important way: the attacker holds the client. They can decompile it, run it on a device they fully control, hook into it at runtime, and bypass anything the app tries to enforce on the device. The topics below cover the fundamentals, the OWASP mobile standards, and the techniques testers use to get past app protections.

HOW IT WORKS

01 Topics

- What is Mobile App Penetration Testing?-: what a mobile pentest covers, why the attacker-holds-the-client model changes everything, and what a report contains.
- Android vs iOS Pentesting: the two platforms have different protections, different tooling, and different common weaknesses. How testing differs.
- What is OWASP MASVS?: the Mobile Application Security Verification Standard. The checklist most mobile pentests are measured against.
- What is OWASP MASTG?: the Mobile Application Security Testing Guide. The how-to manual that pairs with MASVS.
- What is Frida?: the open-source instrumentation toolkit every mobile tester uses to hook into a running app.
- Certificate Pinning Bypass: pinning is meant to stop traffic interception. How testers get past it and why it matters.
- Root and Jailbreak Detection Bypass: apps try to refuse to run on compromised devices. How testers defeat the check and what it really protects.
- Mobile API Testing: most of a mobile app's real attack surface is the API behind it. How to test it properly.

SOURCES

[1] OWASP Mobile Application Security Verification Standard (MASVS)

[2] OWASP Mobile Application Security Testing Guide (MASTG)

[3] OWASP Mobile Top 10

Scope a mobile app penetration test.

securelayer7.net/learn/mobile-security

Open online