

MXS

Mobile eXploitation Specialist

Course Manual



Index

Module 0 — Legal notice and intellectual property.....	1
0. Copyright and conditions of use of the material	1
Module 1 — Introduction to the course	3
1.1. Introduction.....	3
1.2. What is a mobile audit and what parts does it include (app, API and third parties)	4
1.3. How MXS works: mapping, formulating hypotheses, validating and reporting.....	6
1.4. What is reproducible evidence in mobile (request/response + context)	8
1.5. Deliverables that we will build during the course (API map, data map, report)	10
1.6. Ethical framework and scope of responsible use	12
Module 2 — Networks and Internet applied to mobile auditing	13
2.1. IP, gateway, NAT and networks in mobile laboratories.....	13
2.2. Ports and services: how app traffic actually travels.....	16
2.3. DNS and subdomains: API, auth, staging, CDN and usual signals.....	17
2.4. TCP/UDP in practice: timeouts, resets and typical errors	19
2.5. Proxies: why they are the focus of analysis in mobile	20
2.6. Diagnosis: When you don't see traffic, how to locate the problem	22
Module 3 — HTTP/HTTPS and APIs from a Penetration Tester's Perspective	24
3.1. Request/response as a unit of evidence	24
3.2. Routes, parameters, bodies and data models (JSON in practice)	25
3.3. HTTP methods, status codes and signal reading	27
3.4. Common headers and metadata in mobile	28
3.5. Authentication and tokens (access/refresh), expiration and revocation	29
3.6. Authentication vs. Authorization and Why Critical Failures Arise Here	32
3.7. States and sequences in real flows (replay and consistency)	33
3.8. TLS in mobile and particularities of certificates and SDKs.....	35
3.9. WebSockets in mobile applications: handshake, messages and status.....	37
3.10. GraphQL on mobile: queries/mutations, schema and test surface	38
3.11. Other API formats you can find in mobile	40
Module 4 — Environment and tools: the mobile audit workflow	41
4.1. Emulator, simulator and real device: when to use each and how to prepare a useful laboratory	41
4.2. Burp Suite as the center of work: project, listener, scope and operational discipline	43



4.3. Interception and control of traffic in Android/iOS.....	45
4.4. Repeater as a verification and evidence tool.....	47
4.5. Building the API map from real traffic.....	48
4.6. Evidence: what to keep and how to present it.....	50
4.7. Static analysis for pentesters: APK, IPA and signals that feed hypotheses.....	51
4.8. Support tools for triage and analysis.....	52
Module 5 — Server Vulnerabilities.....	54
5.1. How to analyze a vulnerability in the server: signal, hypothesis, test and impact.....	54
5.2. Exposure of insecure information and configurations in the API.....	56
5.3. Manipulation of parameters, states and mass assignment.....	58
5.4. Weak authentication: login, recovery, enumeration, OTP, MFA and delegated biometrics.....	59
5.5. Session and token management: poorly designed reuse, refresh, logout, and JWT.....	60
5.6. Access control: IDOR and authorization broken by object and by action.....	62
5.7. Business logic: states, sequences, limits and functional bypass.....	64
5.8. Rate limiting and resource abuse.....	66
5.9. SQL Injection in Mobile APIs.....	67
5.10. SSRF: when the backend makes requests on behalf of the client.....	68
5.11. Race conditions: concurrency as a vector of abuse.....	69
5.12. Path traversal and unauthorized access to server files.....	70
5.13. Server Side Template Injection.....	71
5.14. Command injection.....	72
5.15. XXE: external entities in XML.....	73
5.16. Open redirect in mobile flows and OAuth.....	74
5.17. CORS misconfigured.....	75
5.18. Insecure deserialization.....	76
5.19. HTTP Parameter Pollution.....	77
5.20. Poorly applied cryptography and poorly designed request signing.....	78
5.21. Module summary and recommended test order.....	80
Module 6 — Application Vulnerabilities.....	81
6.1. What does vulnerability mean in the application and why does it matter.....	81
6.2. Insecure local storage.....	82
6.3. Logs and sensitive data in the console.....	85
6.4. Backups and data extraction.....	86



6.5. Deep links and universal links	88
6.6. WebViews and JavaScript bridges	90
6.7. Exported components and IPC	92
6.8. Analysis of the manifest and platform configuration	93
6.9. Hardcoded secrets and credentials	94
6.10. Clipboard and clipboard exposure.....	95
6.11. Protection of sensitive screens.....	96
6.12. Detection of root or jailbreak and its bypass	97
6.13. Binary Obfuscation and Protection.....	98
6.14. Third-Party SDKs and Data Leaks	99
6.15. Certificate pinning as an analysis surface	100
6.16. Unsafe transport from the application	101
6.17. Module summary and test checklist in the application	102
Module 7 — Professional Report	103
7.1. Structure of a mobile audit report and how to provide value to the right reader	103
7.2. Reproducible evidence and complete finding template	104
7.3. Impact, risk and prioritization.....	107
7.4. Verifiable recommendations and remediation plan.....	108
7.5. API map, data map and authorization matrix as appendices	109
7.6. Presentation of results, defense of the report and preparation for the retest.....	109
Module 8 — Android Security Model for Pentesters	111
8.1. Security architecture: sandbox, UID and isolation	111
8.2. Permissions system and runtime permissions	112
8.3. Components in depth: Activities, Services, Receivers and Providers	113
8.4. Intents, extras, data URI and PendingIntents	114
8.5. Storage, encryption and keystore	116
8.6. APK signing, integrity and repackaging.....	117
8.7. Android version differences relevant to pentesting	117
Module 9 — iOS Security Model for Pentesters.....	118
9.1. Security architecture: sandbox, signature and chain of trust.....	118
9.2. Permissions, privacy and TCC: what the app can request and what it really implies	120
9.3. Info.plist, entitlements and capabilities: declarative decisions that change the surface	121
9.4. Local storage, UserDefaults, files and Keychain	123
9.5. URL schemes, universal links and opening internal flows.....	124



9.6. WebViews, SafariViewController and trust bridges with web content	125
9.7. Transport, certificates and App Transport Security	126
9.8. Integrity, jailbreak, anti-tampering and correct reading of protections.....	128
9.9. Simulator, real device and relevant environmental differences for pentesting.....	129
9.10. Differences by iOS version and compatibility reading in audit.....	130
<i>Module 10 — MXS Exam Preparation</i>	<i>131</i>
10.1. What is actually assessed in the exam and how you should prepare	131
10.2. Time management and work strategy	131
10.3. Common mistakes you should avoid	132
10.4. Mental models for finding vulnerabilities faster	132
10.5. Pre-exam checklist.....	133