

# MXS

Mobile eXploitation Specialist

Manual del curso



## Índice

<b>Módulo 0 — Aviso legal y propiedad intelectual .....</b>	<b>1</b>
0. Copyright y condiciones de uso del material.....	1
<b>Módulo 1 — Introducción al curso .....</b>	<b>3</b>
1.1. Introducción .....	3
1.2. Qué es una auditoría móvil y qué partes incluye (app, API y terceros) .....	4
1.3. Cómo se trabaja en MXS: mapear, plantear hipótesis, validar y reportar .....	6
1.4. Qué es evidencia reproducible en mobile (request/response + contexto) .....	8
1.5. Entregables que construiremos durante el curso (API map, data map, informe).....	10
1.6. Marco ético y alcance de uso responsable .....	12
<b>Módulo 2 — Redes e Internet aplicados a auditoría móvil.....</b>	<b>13</b>
2.1. IP, gateway, NAT y redes en laboratorios móviles .....	13
2.2. Puertos y servicios: cómo viaja realmente el tráfico de una app .....	16
2.3. DNS y subdominios: api, auth, staging, cdn y señales habituales .....	17
2.4. TCP/UDP en la práctica: timeouts, resets y errores típicos.....	19
2.5. Proxies: por qué son el centro del análisis en mobile .....	20
2.6. Diagnóstico: cuando no ves tráfico, cómo localizar el problema.....	22
<b>Módulo 3 — HTTP/HTTPS y APIs desde la perspectiva de un pentester .....</b>	<b>24</b>
3.1. Request/response como unidad de evidencia .....	24
3.2. Rutas, parámetros, cuerpos y modelos de datos (JSON en la práctica) .....	25
3.3. Métodos HTTP, códigos de estado y lectura de señales .....	27
3.4. Cabeceras y metadatos habituales en mobile.....	28
3.5. Autenticación y tokens (access/refresh), caducidad y revocación.....	29
3.6. Autenticación vs autorización y por qué aquí nacen los fallos críticos.....	32
3.7. Estados y secuencias en flujos reales (replay y consistencia) .....	33
3.8. TLS en móvil y particularidades de certificados y SDKs .....	35
3.9. WebSockets en aplicaciones móviles: handshake, mensajes y estado .....	37
3.10. GraphQL en mobile: queries/mutations, esquema y superficie de prueba .....	38
3.11. Otros formatos de API que puedes encontrar en mobile.....	40
<b>Módulo 4 — Entorno y herramientas: el workflow de auditoría móvil .....</b>	<b>41</b>
4.1. Emulador, simulador y dispositivo real: cuándo usar cada uno y cómo preparar un laboratorio útil.....	41
4.2. Burp Suite como centro del trabajo: proyecto, listener, scope y disciplina operativa .....	43



4.3. Interceptación y control del tráfico en Android/iOS .....	45
4.4. Repeater como herramienta de verificación y evidencia.....	47
4.5. Construcción del API map desde tráfico real.....	48
4.6. Evidencias: qué guardar y cómo presentarlo .....	50
4.7. Análisis estático para pentesters: APK, IPA y señales que alimentan hipótesis .....	51
4.8. Herramientas de apoyo para triage y análisis.....	52
<b>Módulo 5 — Vulnerabilidades en el servidor.....</b>	<b>54</b>
5.1. Cómo analizar una vulnerabilidad en el servidor: señal, hipótesis, prueba e impacto.....	54
5.2. Exposición de información y configuraciones inseguras en la API.....	57
5.3. Manipulación de parámetros, estados y mass assignment.....	58
5.4. Autenticación débil: login, recuperación, enumeración, OTP, MFA y biometría delegada.....	59
5.5. Gestión de sesión y tokens: reuso, refresh, logout y JWT mal diseñados .....	61
5.6. Control de acceso: IDOR y autorización rota por objeto y por acción.....	63
5.7. Lógica de negocio: estados, secuencias, límites y bypass funcional .....	64
5.8. Rate limiting y abuso de recursos .....	66
5.9. Inyección SQL en APIs móviles.....	67
5.10. SSRF: cuando el backend hace peticiones por el cliente .....	69
5.11. Race conditions: concurrencia como vector de abuso .....	70
5.12. Path traversal y acceso indebido a ficheros del servidor .....	71
5.13. Server Side Template Injection .....	72
5.14. Command injection.....	73
5.15. XXE: entidades externas en XML.....	74
5.16. Open redirect en flujos móviles y OAuth .....	75
5.17. CORS mal configurado .....	76
5.18. Insecure deserialization .....	77
5.19. HTTP Parameter Pollution.....	78
5.20. Criptografía mal aplicada y request signing mal diseñado .....	79
5.21. Resumen del módulo y orden de pruebas recomendado .....	81
<b>Módulo 6 — Vulnerabilidades en la aplicación.....</b>	<b>82</b>
6.1. Qué significa vulnerabilidad en la aplicación y por qué importa.....	82
6.2. Almacenamiento local inseguro .....	83
6.3. Logs y datos sensibles en consola .....	86
6.4. Backups y extracción de datos .....	87
6.5. Deep links y universal links .....	89



6.6. WebViews y bridges JavaScript.....	91
6.7. Componentes exportados e IPC .....	93
6.8. Análisis del manifiesto y de la configuración de plataforma .....	94
6.9. Secretos y credenciales hardcodeados .....	96
6.10. Clipboard y exposición en portapapeles.....	97
6.11. Protección de pantallas sensibles .....	98
6.12. Detección de root o jailbreak y su bypass .....	99
6.13. Ofuscación y protección del binario .....	100
6.14. SDKs de terceros y fugas de datos .....	101
6.15. Certificate pinning como superficie de análisis .....	102
6.16. Transporte inseguro desde la aplicación .....	103
6.17. Resumen del módulo y checklist de pruebas en la aplicación .....	104
<b>Módulo 7 — Informe profesional.....</b>	<b>105</b>
7.1. Estructura de un informe de auditoría móvil y cómo darle valor al lector correcto.....	105
7.2. Evidencia reproducible y plantilla completa de hallazgo .....	106
7.3. Impacto, riesgo y priorización.....	109
7.4. Recomendaciones verificables y plan de remediación .....	109
7.5. API map, data map y matriz de autorización como anexos .....	110
7.6. Presentación de resultados, defensa del informe y preparación del retest.....	111
<b>Módulo 8 — Modelo de seguridad de Android para pentesters.....</b>	<b>112</b>
8.1. Arquitectura de seguridad: sandbox, UID y aislamiento .....	112
8.2. Sistema de permisos y runtime permissions.....	113
8.3. Componentes en profundidad: Activities, Services, Receivers y Providers.....	114
8.4. Intents, extras, data URI y PendingIntents .....	115
8.5. Almacenamiento, cifrado y keystore .....	117
8.6. Firma de APK, integridad y reempaquetado.....	118
8.7. Diferencias por versión de Android relevantes para pentesting .....	118
<b>Módulo 9 — Modelo de seguridad de iOS para pentesters .....</b>	<b>119</b>
9.1. Arquitectura de seguridad: sandbox, firma y cadena de confianza.....	119
9.2. Permisos, privacidad y TCC: qué puede pedir la app y qué implica realmente.....	121
9.3. Info.plist, entitlements y capacidades: decisiones declarativas que cambian la superficie .....	122
9.4. Almacenamiento local, UserDefaults, archivos y Keychain .....	124
9.5. URL schemes, universal links y apertura de flujos internos .....	125

---

9.6. WebViews, SafariViewController y puentes de confianza con contenido web .....	126
9.7. Transporte, certificados y App Transport Security .....	128
9.8. Integridad, jailbreak, anti-tampering y lectura correcta de las protecciones .....	129
9.9. Simulador, dispositivo real y diferencias de entorno relevantes para pentesting .....	130
9.10. Diferencias por versión de iOS y lectura de compatibilidad en auditoría .....	131
<b>Módulo 10 — Preparación para el examen MXS.....</b>	<b>132</b>
10.1. Qué se evalúa realmente en el examen y cómo debes prepararte .....	132
10.2. Gestión del tiempo y estrategia de trabajo .....	133
10.3. Errores comunes que debes evitar .....	133
10.4. Modelos mentales para encontrar hallazgos más rápido .....	134
10.5. Checklist pre examen .....	135