

WXE

Web eXploitation Expert

Manual del curso



Índice

Módulo 0 — Aviso legal y propiedad intelectual	1
0. Copyright y condiciones de uso del material	1
Módulo 1 — Mentalidad Bug Bounty y metodología experta	3
1.1. Qué es “impacto” en Bug Bounty.....	3
1.2. Reglas de programa: scope, out-of-scope, safe harbor	5
1.3. Flujo: recon → hipótesis → prueba → impacto → reporte.....	7
1.4. Priorización por señales.....	9
1.5. Cómo reducir duplicados	11
1.6. Cadenas de impacto (chaining) con criterio	13
1.7. Sistema de notas y trazabilidad	15
Módulo 2 — Recon avanzado y attack surface real	17
2.1. Modelo de superficie: activos, roles, datos, integraciones.....	17
2.2. Subdominios y entornos (prod/stage/dev)	19
2.3. Content discovery con intención	21
2.4. Parameter mining y features ocultas	23
2.5. Fingerprinting útil (CDN/WAF/framework/APIs)	25
2.6. Roles y permisos inferidos por comportamiento	27
2.7. Recon orientado a impacto.....	29
Módulo 3 — Mapping moderno con JavaScript y SPAs	31
3.1. Por qué el JS decide la superficie	31
3.2. Extracción de endpoints desde bundles/sourcemaps	33
3.3. Separar API real de ruido del front.....	35
3.4. Tokens, configs y feature flags expuestos.....	37
3.5. Flujos SPA: estados y acciones.....	39
3.6. Errores SPA que abren bugs server-side	41
Módulo 4 — Arquitectura real: CDN, proxy, WAF y caché	43
4.1. Capas típicas en producción.....	43
4.2. Normalización de rutas y encoding entre capas.....	45
4.3. Cabeceras críticas (Host, X-Forwarded-*, Origin, Vary)	47
4.4. Señales de WAF y testing responsable.....	49
4.5. Observabilidad básica (timing, códigos, redirects).....	51
4.6. Riesgos por desacuerdo entre capas	52

Módulo 5 — HTTP Request Smuggling y desync.....	55
5.1. Modelo mental de desync.....	55
5.2. Parsing: Content-Length vs Transfer-Encoding.....	57
5.3. Tipos de desync y señales	59
5.4. Detección segura y reproducible.....	61
5.5. Validación de impacto (bypass/auth/poisoning).....	63
5.6. Falsos positivos y cómo descartarlos.....	65
5.7. Mitigaciones y hardening.....	66
Módulo 6 — Web Cache Poisoning y Cache Deception	68
6.1. Keying, Vary y unkeyed inputs.....	68
6.2. Web Cache Poisoning: vectores comunes.....	71
6.3. Cache Deception: rutas/extensiones/reglas	73
6.4. Señales prácticas (hits/misses, TTL)	75
6.5. Validación de impacto y alcance.....	77
6.6. Errores típicos de reporte.....	79
6.7. Mitigaciones (público/privado, bypass cache).....	81
Módulo 7 — Host Header, CRLF y ataques de cabeceras	83
7.1. Host header injection: condiciones reales	83
7.2. Password reset poisoning.....	85
7.3. X-Forwarded-Host y variantes	87
7.4. CRLF / response splitting: conceptos y detección segura	88
7.5. Relación con cache/redirects	90
7.6. Mitigaciones.....	92
Módulo 8 — API Hacking profesional (REST)	93
8.1. Mentalidad API: recursos, acciones, objetos	93
8.2. BOLA/IDOR avanzado en APIs.....	96
8.3. Broken Function Level Authorization.....	98
8.4. Excessive Data Exposure	100
8.5. Mass Assignment (overposting).....	102
8.6. Improper Inventory (legacy/versioning).....	104
8.7. Rate limiting y anti-automation en APIs	105
Módulo 9 — GraphQL Security aplicado.....	107
9.1. Cómo se piensa un schema	107



9.2. Introspection y discovery “reportable”	110
9.3. Autorización por resolver	112
9.4. BOLA en queries/mutations.....	113
9.5. Leakage por errores y mensajes	115
9.6. Complejidad/profundidad (riesgo DoS responsable)	117
9.7. Mitigaciones.....	119
Módulo 10 — WebSockets y real-time security.....	120
10.1. Handshake: cookies/tokens/origen	120
10.2. Autorización por canal y por evento.....	122
10.3. CSWSH (Cross-Site WebSocket Hijacking)	125
10.4. Multi-tenant en tiempo real.....	127
10.5. Mitigaciones	129
Módulo 11 — Auth moderna y SSO (JWT, OAuth2/OIDC, SAML)	130
11.1. Modelos de sesión modernos y lifecycle.....	130
11.2. JWT: validación correcta y fallos típicos	132
11.3. Token leakage: vectores comunes.....	134
11.4. OAuth2/OIDC: lo mínimo para auditar bien	136
11.5. Errores típicos (redirect_uri, state, nonce, PKCE).....	139
11.6. ATO por flujo (reset/cambio email/magic links).....	141
11.7. SAML: fallos frecuentes de validación	143
11.8. Mitigaciones	145
Módulo 12 — Client-side avanzado (DOM, proto, mensajes)	147
12.1. DOM XSS moderno: sinks y sanitización.....	147
12.2. Contextos y encoding avanzados.....	148
12.3. Prototype Pollution: de bug a impacto.....	151
12.4. postMessage: origin y data handling	153
12.5. window.opener y tabnabbing	156
12.6. Clickjacking y frame-ancestors.....	157
12.7. Introducción práctica a XS-Leaks.....	159
Módulo 13 — Inyecciones avanzadas y explotación controlada	161
13.1. NoSQL Injection.....	161
13.2. LDAP Injection.....	163
13.3. XPath Injection.....	165



13.4. SSTI avanzado (contexto/sandbox/impacto)	167
13.5. Deserialización insegura (señales y validación responsable)	169
13.6. ReDoS (criterios de reportabilidad)	172
13.7. Mitigaciones	174
Módulo 14 — Business Logic Expert (race, estados, multi-tenant)	175
14.1. Lectura de flujos de negocio	175
14.2. State machines y saltos de estado	177
14.3. Race conditions y TOCTOU	180
14.4. Límites y rate limiting por diseño (bypass)	182
14.5. Multi-tenant: aislamiento por organización	184
14.6. Impacto en negocio (fraude/abuso/escalada)	186
14.7. Mitigación	188
Módulo 15 — Cloud y terceros (SSRF impacto, takeover, secretos)	189
15.1. SSRF en cloud: cuándo llega a metadata	189
15.2. Impacto cloud reportable (credenciales temporales)	191
15.3. Subdomain takeover	193
15.4. Secretos expuestos (front/repos/artefactos)	195
15.5. Mitigaciones	198
Módulo 16 — Reporting que pasa triage	199
16.1. Estructura de reporte “triage-proof”	199
16.2. Evidencias obligatorias y reproducibilidad	201
16.3. Impacto y riesgo sin relleno	203
16.4. Duplicados: diferenciadores y alcance	205
16.5. Recomendaciones verificables	206
16.6. Comunicación con triagers y seguimiento	208