

# WXE

Web eXploitation Expert

Course Manual





## Index

<b>Module 0 — Legal notice and intellectual property</b> .....	<b>1</b>
0. Copyright and conditions of use of the material.....	1
<b>Module 1 — Bug Bounty Mindset and Expert Methodology</b> .....	<b>3</b>
1.1. What is “impact” in Bug Bounty .....	3
1.2. Program rules: scope, out-of-scope, safe harbor .....	5
1.3. Flow: reconnaissance → hypothesis → test → impact → report.....	7
1.4. Signal prioritization.....	9
1.5. How to reduce duplicates.....	11
1.6. Impact chains with criteria.....	13
1.7. Notes and traceability system .....	15
<b>Module 2 —Advanced reconnaissance and real surface attack</b> .....	<b>17</b>
2.1. Surface model: assets, roles, data, integrations .....	17
2.2. Subdomains and environments (prod/stage/dev) .....	19
2.3. Content discovery with intention.....	21
2.4. Parameter mining and hidden features .....	23
2.5. Useful fingerprinting (CDN/WAF/framework/APIs) .....	25
2.6. Roles and permissions inferred by behavior .....	27
2.7. Impact-oriented reconnaissance.....	29
<b>Module 3 — Modern Mapping with JavaScript and SPAs</b> .....	<b>31</b>
3.1. Why the JS decides the surface.....	31
3.2. Extracting endpoints from bundles/sourcemaps.....	33
3.3. Separate real API from front-end noise .....	35
3.4. Exposed tokens, configs and feature flags.....	37
3.5. SPA Flows: States and Actions .....	39
3.6. SPA errors that open server-side bugs .....	41
<b>Module 4 — Real Architecture: CDN, proxy, WAF and cache</b> .....	<b>43</b>
4.1. Typical layers in production .....	43
4.2. Normalization of routes and encoding between layers .....	45
4.3. Critical Headers (Host, X-Forwarded-*, Origin, Vary) .....	47
4.4. WAF signals and responsible testing.....	49
4.5. Basic observability (timing, codes, redirects) .....	51
4.6. Risks due to disagreement between layers .....	52



---

<b>Module 5 — HTTP Request Smuggling and desync .....</b>	<b>55</b>
5.1. Mental model of desync .....	55
5.2. Parsing: Content-Length vs Transfer-Encoding.....	57
5.3. Types of desync and signals .....	59
5.4. Safe and reproducible detection.....	61
5.5. Impact validation (bypass/auth/poisoning).....	63
5.6. False positives and how to rule them out .....	65
5.7. Mitigations and hardening.....	66
<b>Module 6 — Web Cache Poisoning and Cache Deception .....</b>	<b>68</b>
6.1. Keying, Vary and unlocked inputs.....	68
6.2. Web Cache Poisoning: Common Vectors .....	71
6.3. Cache Deception: routes/extensions/rules .....	73
6.4. Practical signals (hits/misses, TTL) .....	75
6.5. Impact and scope validation .....	77
6.6. Typical reporting errors.....	79
6.7. Mitigations (public/private, cache bypass) .....	81
<b>Module 7 — Host Header, CRLF and Header Attacks .....</b>	<b>83</b>
7.1. Host header injection: real conditions .....	83
7.2. Password reset poisoning.....	85
7.3. X-Forwarded-Host and variants .....	87
7.4. CRLF / response splitting: concepts and secure detection .....	89
7.5. Relationship with cache/redirects .....	90
7.6. Mitigations .....	92
<b>Module 8 — Professional API Hacking (REST) .....</b>	<b>93</b>
8.1. API Mindset: Resources, Actions, Objects .....	93
8.2. Advanced BALL/IDOR in 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 and anti-automation in APIs.....	106
<b>Module 9 — GraphQL Security applied.....</b>	<b>107</b>
9.1. How to think about a schema.....	107



---

9.2. Introspection and “reportable” discovery.....	110
9.3. Authorization pending resolution .....	112
9.4. BALL in queries/mutations .....	114
9.5. Leakage due to errors and messages .....	116
9.6. Complexity/depth (responsible DoS risk) .....	117
9.7. Mitigations .....	119
<b>Module 10 — WebSockets and real-time security.....</b>	<b>120</b>
10.1. Handshake: cookies/tokens/origin.....	120
10.2. Authorization by channel and by event.....	123
10.3. CSWSH (Cross-Site WebSocket Hijacking) .....	125
10.4. Real-time multi-tenant.....	128
10.5. Mitigations.....	130
<b>Module 11 — Modern Auth and SSO (JWT, OAuth2/OIDC, SAML).....</b>	<b>131</b>
11.1. Modern session models and lifecycle .....	131
11.2. JWT: successful validation and typical failures.....	133
11.3. Token leakage: common vectors.....	135
11.4. OAuth2/OIDC: the minimum for good auditing .....	137
11.5. Typical errors (redirect_uri, state, nonce, PKCE) .....	140
11.6. ATO by flow (reset/change email/magic links).....	142
11.7. SAML: Frequent validation failures.....	144
11.8. Mitigations.....	147
<b>Module 12 — Advanced Client-side (DOM, proto, messages).....</b>	<b>148</b>
12.1. Modern DOM XSS: Sinks and Sanitation.....	148
12.2. Advanced Contexts and Encoding.....	150
12.3. Prototype Pollution: from bug to impact.....	152
12.4. postMessage: origin and data handling .....	155
12.5. window.opener and tabnabbing .....	157
12.6. Clickjacking and frame-ancestors .....	159
12.7. Practical Introduction to XS-Leaks.....	161
<b>Module 13 — Advanced Injections and Controlled Exploitation.....</b>	<b>163</b>
13.1. NoSQL Injection.....	163
13.2. LDAP Injection.....	165
13.3. XPath Injection.....	167



---

13.4. Advanced SSTI (context/sandbox/impact) .....	168
13.5. Insecure Deserialization (Signals and Responsible Validation) .....	171
13.6. ReDoS (reportability criteria).....	173
13.7. Mitigations.....	175
<b>Module 14 — Business Logic Expert (race, states, multi-tenant).....</b>	<b>176</b>
14.1. Reading business flows .....	176
14.2. State machines and state jumps .....	179
14.3. Race conditions and TOCTOU.....	181
14.4. Limits and rate limiting by design (bypass).....	183
14.5. Multi-tenant: Isolation by Organization .....	185
14.6. Impact on business (fraud/abuse/escalation).....	187
14.7. Mitigation.....	189
<b>Module 15 — Cloud and third parties (SSRF impact, takeover, secrets).....</b>	<b>191</b>
15.1. SSRF in the cloud: when it reaches metadata .....	191
15.2. Reportable cloud impact (temporary credentials).....	193
15.3. Subdomain takeover .....	195
15.4. Exposed Secrets (front/repos/artifacts).....	197
15.5. Mitigations.....	199
<b>Module 16 — Reporting that goes through triage .....</b>	<b>201</b>
16.1. Triage-proof report structure.....	201
16.2. Mandatory evidence and reproducibility .....	202
16.3. Impact and risk without filler .....	204
16.4. Duplicates: differentiators and scope .....	206
16.5. Verifiable recommendations.....	208
16.6. Communication with triagers and follow-up .....	210