



# WXJ

## Web eXploitation Junior

### Course Manual





## Índice

<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 — Introduction to the course</b> .....	<b>3</b>
1. Introduction.....	3
<b>Module 2 — Networks and Internet</b> .....	<b>5</b>
2.1. Network, IP, gateway, private networks and localhost.....	5
2.2. Ports and services.....	6
2.3. DNS.....	7
2.4. TCP and UDP .....	9
2.5. Web communication flow: from URL to response.....	10
2.6. Network-level access control: service exposure and filtering.....	11
2.7. Proxy and web traffic.....	12
2.8. Connectivity verification and diagnosis .....	13
<b>Module 3 — Fundamentals of HTTP/HTTPS and web communication</b> .....	<b>16</b>
3.1. URLs, routes, endpoints and parameters.....	16
3.2. Structure of a request and a response .....	17
3.3. HTTP Methods and Semantics .....	19
3.4. State codes and their interpretation .....	21
3.5. HTTP Headers .....	22
3.6. Request body and usual formats .....	24
3.7. Cookies and sessions .....	25
3.8. Authentication and authorization.....	27
3.9. Redirections, common flows and actual navigation .....	28
3.10. Dynamic Content and APIs: HTML vs JSON .....	30
3.11. Same-Origin Policy and CORS.....	31
3.12. Cache, compression and effects on auditing .....	32
3.13. HTTPS/TLS .....	34
3.14. Standardization and coding.....	35
3.15. Preparation for proxy analysis.....	37
<b>Module 4 — Web Audit Environment and Tools</b> .....	<b>38</b>
4.1. Environment Preparation.....	38
4.2. Burp Suite Community: Installation and Initial Verification .....	40



4.3. Sending browser traffic to Burp (Firefox + FoxyProxy) .....	42
4.4. Intercept: control of the flow of requests .....	47
4.5. Scope and organization of the project .....	51
4.6. Repeater: controlled reproduction and modification of requests .....	53
4.7. Intruder: controlled tests, dictionaries and reading results .....	55
4.8. Decoder/Encoder: URL encoding, Base64 and common transformations .....	58
4.9. Comparer: comparison of responses and detection of relevant differences .....	60
4.10. Supporting tools: DevTools, curl, Wappalyzer and proxy alternatives .....	62
4.11. Export of evidence.....	65
<b>Module 5 — Fundamental Web Vulnerabilities.....</b>	<b>67</b>
5.1. How to analyze a vulnerability.....	67
5.2. Exposure of insecure information and configurations .....	68
5.3. Unvalidated input and parameter tampering.....	70
5.4. Authentication: common failures.....	72
5.5. Account recovery and password reset (typical errors) .....	74
5.6. Business Logic Errors .....	76
5.7. Access control: IDOR and broken authorization .....	78
5.8. Session management: cookies and security attributes.....	80
5.9. XSS (Cross-Site Scripting).....	82
5.10. CSRF and modern defenses.....	85
5.11. CORS misconfigured .....	88
5.12. SQL Fundamentals for Web Auditing.....	90
5.13. SQL Injection (SQLi).....	92
5.14. Path Traversal and LFI .....	94
5.15. Insecure file upload .....	96
5.16. XML and XXE .....	99
5.17. SSRF (Server-Side Request Forgery).....	101
5.18. SSTI (Server-Side Template Injection).....	103
5.19. Command Injection.....	105
5.20. Open Redirect.....	107
5.21. Module summary and checklist.....	109
<b>Module 6 — Professional Report and Closing an Audit .....</b>	<b>112</b>
6.1. Purpose of the report and principles of technical communication .....	112
6.2. Complete structure of a web audit report.....	113



---

<b>6.3. Writing findings: standard format, evidence and reproducible PoC .....</b>	<b>116</b>
<b>6.4. Severity and prioritization: impact, probability and CVSS .....</b>	<b>117</b>
<b>6.5. Recommendations and remediation plan: how to propose useful solutions .....</b>	<b>119</b>
<b>6.6. Annexes and delivery: evidence, traceability, version control and good practices .....</b>	<b>120</b>