



WXJ

Web eXploitation Junior

Manual del curso





Índice

Módulo 0 — Aviso legal y propiedad intelectual	1
0. Copyright y condiciones de uso del material	1
Módulo 1 — Introducción al curso	3
1. Introducción.....	3
Módulo 2 — Redes e Internet	5
2.1. Red, IP, gateway, redes privadas y localhost	5
2.2. Puertos y servicios.....	6
2.3. DNS.....	7
2.4. TCP y UDP	8
2.5. Flujo de comunicación web: de URL a respuesta.....	10
2.6. Control de acceso a nivel de red: exposición de servicios y filtrado	11
2.7. Proxy y tráfico web.....	12
2.8. Verificación y diagnóstico de conectividad.....	13
Módulo 3 — Fundamentos de HTTP/HTTPS y comunicación web	16
3.1. URLs, rutas, endpoints y parámetros	16
3.2. Estructura de una petición y una respuesta	17
3.3. Métodos HTTP y semántica	19
3.4. Códigos de estado y su interpretación.....	21
3.5. Cabeceras HTTP.....	22
3.6. Cuerpo de la petición y formatos habituales	24
3.7. Cookies y sesiones	25
3.8. Autenticación y autorización	27
3.9. Redirecciones, flujos comunes y navegación real.....	28
3.10. Contenido dinámico y APIs: HTML vs JSON.....	30
3.11. Same-Origin Policy y CORS.....	31
3.12. Caché, compresión y efectos en auditoría.....	33
3.13. HTTPS/TLS	34
3.14. Normalización y codificaciones	36
3.15. Preparación para el análisis con proxy	37
Módulo 4 — Entorno y herramientas de auditoría web	39
4.1. Preparación del entorno	39
4.2. Burp Suite Community: instalación y verificación inicial	40



4.3. Envío de tráfico del navegador a Burp (Firefox + FoxyProxy)	43
4.4. Intercept: control del flujo de peticiones.....	48
4.5. Scope y organización del proyecto.....	52
4.6. Repeater: reproducción y modificación controlada de peticiones	54
4.7. Intruder: pruebas controladas, diccionarios y lectura de resultados	56
4.8. Decoder/Encoder: URL encoding, Base64 y transformaciones comunes.....	59
4.9. Comparer: comparación de respuestas y detección de diferencias relevantes	61
4.10. Herramientas de apoyo: DevTools, curl, Wappalyzer y alternativas de proxy	63
4.11. Exportación de evidencias	66
Módulo 5 — Vulnerabilidades web fundamentales	68
5.1. Cómo analizar una vulnerabilidad.....	68
5.2. Exposición de información y configuraciones inseguras	69
5.3. Entrada no validada y parameter tampering	71
5.4. Autenticación: fallos comunes.....	73
5.5. Recuperación de cuenta y restablecimiento de contraseña (errores típicos).....	76
5.6. Errores de lógica de negocio (Business Logic Errors).....	77
5.7. Control de acceso: IDOR y autorización rota	80
5.8. Gestión de sesión: cookies y atributos de seguridad	82
5.9. XSS (Cross-Site Scripting).....	84
5.10. CSRF y defensas modernas.....	87
5.11. CORS mal configurado	89
5.12. Fundamentos de SQL para auditoría web	91
5.13. SQL Injection (SQLi).....	93
5.14. Path Traversal y LFI.....	95
5.15. Subida de archivos insegura.....	97
5.16. XML y XXE.....	100
5.17. SSRF (Server-Side Request Forgery).....	102
5.18. SSTI (Server-Side Template Injection).....	104
5.19. Command Injection.....	106
5.20. Open Redirect.....	108
5.21. Resumen del módulo y checklist.....	110
Módulo 6 — Informe profesional y cierre de una auditoría.....	113
6.1. Finalidad del informe y principios de comunicación técnica	113
6.2. Estructura completa de un informe de auditoría web	115



6.3. Redacción de hallazgos: formato estándar, evidencia y PoC reproducible.....	117
6.4. Severidad y priorización: impacto, probabilidad y CVSS	119
6.5. Recomendaciones y plan de remediación: cómo proponer soluciones útiles	121
6.6. Anexos y entrega: evidencias, trazabilidad, control de versiones y buenas prácticas.....	122