

Programación Web Segura, OWASP (incluye OWASP Top 10 for LLM Applications IA)

Temario

1. Principios del Diseño de Software Seguro
 - 1.1. Conceptos generales sobre el desarrollo de aplicaciones web
 - 1.2. OWASP Top 10, CWE y SANS Top 20
 - 1.3. Guía de desarrollo de OWASP
 - 1.4. Open Source Security Testing Methodology Manual (OSSTMM)
2. Nociones de HTTP
 - 2.1. Peticiones/Respuestas
 - 2.2. Cookies
 - 2.3. Referer
3. Herramientas para Analizar Tráfico
 - 3.1. Firebug
 - 3.2. TamperIE
 - 3.3. WebKit Web Inspector
 - 3.4. WebScarab
 - 3.5. Fiddler
 - 3.6. Wireshark
 - 3.7. Proxies HTTP
4. Fuga de Información
 - 4.1. Páginas de error
 - 4.2. Comentarios
5. Validaciones
6. Open Web Application Security Project (OWASP) 2021
 - 6.1. A1-Broken Access Control
 - 6.2. A2-Cryptographic Failures
 - 6.3. A3-Injection
 - 6.4. A4-Insecure Design
 - 6.5. A5-Security Misconfiguration
 - 6.6. A6-Vulnerable and Outdated Components
 - 6.7. A7-Identification and Authentication Failures
 - 6.8. A8-Software and Data Integrity Failures
 - 6.9. A9-Security Logging and Monitoring Failures
 - 6.10. A10 Server Side Request Forgery
7. Open Web Mobile Application Security Project
8. OWASP Top 10 for LLM Applications IA
9. Frameworks para Programación Web Segura
 - 9.1. Spring Security
 - 9.2. ESAPI y OWASP Java Encoder
 - 9.3. Security Hardening en el servidor
10. Herramientas
 - 10.1. Para detectar vulnerabilidades en el software
 - 10.2. De tráfico de red