Programación Web Segura (OWASP)

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) 2017
    6.1. A1-Injection
    6.2. A2-Broken Authentication
    6.3. A3-Sensitive Data Exposure
    6.4. A4-XML External Entities (XXE)
    6.5. A5-Broken Access Control
    6.6. A6-Security Misconfiguration
    6.7. A7-Cross-Site Scripting (XSS)
    6.8. A8-Insecure Deserialization
    6.9. A9-Using Components with Known Vulnerabilities
    6.10. A10-Insufficient Logging & Monitoring

7. Open Web Mobile Application Secutity Project 2016

8. Frameworks para Programación Web Segura
    8.1. Spring Security
    8.2. HDIV
    8.3. ESAPI JavaScript Edition
    8.4. jQuery-encoder
    8.5. Security Hardening en el servidor

9. Herramientas
    9.1. Para detectar vulnerabilidades en el software
    9.2. De trafico de red