Curso Metodología de desarrollo seguro

Temario

1.Principios del diseño de software seguro
Conceptos generales sobre el desarrollo de aplicaciones web
OWASP Top 10, CWE y SANS Top 20
Guía de desarrollo de OWASP
Open Source Security Testing Methodology Manual (OSSTMM)

2.Nociones de HTTP
Peticiones/Respuestas
Cookies
Referer

3.Herramientas para analizar tráfco
Firebug
TamperIE
WebKit Web Inspector
WebScarab
Fiddler
Wireshark
Proxies HTTP

4.Fuga de información
Páginas de error
Comentarios

5.Validaciones

6.Open Web Application Security Project (OWASP) 2017
A1-Injection
A2-Broken Authentication
A3-Sensitive Data Exposure
A4-XML External Entities (XXE)
A5-Broken Access Control
A6-Security Misconfiguration
A7-Cross-Site Scripting (XSS)
A8-Insecure Deserialization
A9-Using Components with Known Vulnerabilities
A10-Insufficient Logging&Monitoring

7.Open Web Mobile Application Secutity Project 2016

M1-Improper PlatformUsage
M2-Insecure Data Storage
M3-Insecure Communication
M4-Insecure Authentication
M5-Insufficient Cryptography
M6-Insecure Authorization
M7-Poor CodeQuality
M8-Code Tampering
M9-Reverse Engineering
M10-Extraneous Functionality

8.Frameworks para programación web segura

Spring Security
HDIV
ESAPI JavaScript Edition
jQuery-encoder
Security Hardening en el servidor

9.Herramientas

Para detectar vulnerabilidades en el software
De trafico de red