

Seguridad aplicaciones Java

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
 - 1.3.1. Análisis estático
 - 1.3.2. Análisis dinámico
 - 1.3.3. Todo bajo control: Checklist
2. Nociones de HTTP
 - 2.1. Peticiones/Respuestas
 - 2.2. Cookies
 - 2.3. Referer
3. Herramientas para analizar tráfico
 - 3.1. Firebug
 - 3.2. Proxies HTTP
4. Fuga de información
 - 4.1. Páginas de error
 - 4.2. Comentarios
5. Validaciones
6. Open Web Application Security Project (OWASP)
 - 6.1. Testing Black y White Box
 - 6.2. Tipos de validaciones
 - 6.3. A1. Ataques de inyección
 - 6.3.1. Comandos de sistema operativo
 - 6.3.2. SQL Injection y Blind SQL Injection
 - 6.3.3. LDAP
 - 6.3.4. Xpath y JSON
 - 6.4. A2. Cross-site Scripting (XSS)
 - Tipos y definiciones
 - 6.4.2. Técnicas de inyección de script
 - 6.4.3. Codificación y ofuscamiento
 - 6.4.4. Prevención de inyecciones
 - 6.5. A3. Autenticación y gestión de sesiones
 - 6.5.1. Cookies inseguras
 - 6.5.2. Validación de sesión y pérdida de autenticación (Session Fixation)
 - 6.6. A4. Referencia insegura directa a objetos
 - 6.6.1. Redirecciones y restricciones de acceso
 - 6.6.2. Rutas por defecto e inseguras
 - 6.6.3. Path traversal
 - 6.6.4. Codificación y uso de Null bytes
 - 6.7. A5. Falsificación de petición - Cross_Site_Request_Forgery (CSRF)
 - 6.8. A6. Configuración defectuosa y/o por defecto de aplicaciones y objetos
 - 6.8.1. Directorios por defecto

- 6.8.2. Archivos de configuración
 - 6.8.3. Backups
 - 6.8.4. Base de datos
- 6.9. A7. Almacenamiento criptográfico inseguro
 - 6.9.1. Generación de contraseñas en aplicaciones
 - 6.9.2. Hashing
 - 6.9.3. HMAC
 - 6.9.4. OpenId
- 6.10. A8. Falla de restricción de acceso a sitios web y su configuración adecuada
- 6.11. A9. Validación de capa de transporte
 - 6.11.1. Certificados digitales
 - 6.11.2. Protocolo HTTPS
- 6.12. A10. Redirecciones no validadas
- 6.13. Frameworks para programación web segura
 - 6.13.1. Spring Security
 - 6.13.2. HDIV
 - 6.13.3. ESAPI JavaScript Edition
 - 6.13.4. jQuery-encoder
- 6.14. Security Hardening en el servidor
- 7. Open Web Mobile Application Security Project 2023
 - 7.1. M1: Improper Credential Usage
 - 7.2. M2: Inadequate Supply Chain Security
 - 7.3. M3: Insecure Authentication/Authorization
 - 7.4. M4: Insufficient Input/Output Validation
 - 7.5. M5: Insecure Communication
 - 7.6. M6: Inadequate Privacy Controls
 - 7.7. M7: Insufficient Binary Protections
 - 7.8. M8: Security Misconfiguration
 - 7.9. M9: Insecure Data Storage
 - 7.10. M10: Insufficient Cryptography
- 8. Frameworks para programación web segura
 - 8.1. Spring Security
 - 8.2. ESAPI JavaScript Edition
 - 8.3. Security Hardening en el servidor