Desarrollo seguro de Aplicaciones Web basado en OWASP

Por: Carlos Carreño,

OCP, ScrumMaster, Solution Architect

Email: ccarrenovi@Gmail.com

Unidad 1 Introducción a la seguridad en el desarrollo de software

- Casos reales de vulnerabilidades y su impacto.
- Problemática de las aplicaciones inseguras.
- La Seguridad Informática en el desarrollo del software.

Autor: ccarrenovi@Gmail.com

Casos reales de vulnerabilidades y su impacto.

- **Wannacry**, 12 de Mayo del 2017, Malware, 4,000 millones de Euros
- **Conficker**, Octubre 2008, Gusano, 190 países, 10 millones de Equipos
- **Stuxnet**, Verano 2010, Malware, Retraso el programa nuclear Iraní
- **Petya**, 2016, 2017 (**NotPetya**) El impacto económico no ha podido ser calculado
- **ILoveYOU**, 2001, Infecto Correo, impacto 1,200 millones de dólares

Problemática de las aplicaciones inseguras.

- De 14 aplicaciones móviles de Banca con mas de 500,000 (medio millón de descargas) se detecto:
  - El 29% de las aplicaciones bancarias de Android contenían fallas de alto riesgo.
  - El 46% de los problemas fueron detectadas en lado cliente, de estos el 76% no requería tener acceso al dispositivo físico.
  - El 80% de las aplicaciones tenia acceso no autorizado del lado cliente.
  - Vulnerabilidades “Acceso no autorizado”, “Ataque de man-in-the-middle”

Fuente:
https://www.techrepublic.com/article/popular-mobile-banking-apps-are-riddled-with-security-flaws-and-android-users-are-more-at-risk/

La Seguridad Informática en el desarrollo del software.

- Principios fundamentales:
  - Integridad
  - Confidencialidad
  - Disponibilidad
  - No repudio
  - Autenticación o autenticidad
- Estándares de Seguridad
  - ISO 17799
  - ISO/IEC 27000
  - ISO/IEC 27000: 2014 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Generalidades y vocabulario
  - ISO/IEC 27001:2013 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información – Requisitos
  - ISO/IEC 27002:2013 Tecnología de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información
  - “OWASP (Open Web Application Security Project)

La Seguridad Informática en el desarrollo del software.

- Estándares y normas para la Ingeniería de Requisitos
  - **OWASP Testing Framework WSTG – v4-1**
    - El objetivo del proyecto es ayudar a las personas a comprender el *qué* , *por qué* , *cuándo* , *dónde* y *cómo* probar aplicaciones web
  - ISO 29148 – Ingeniería de sistemas y software - Procesos del ciclo de vida - Ingeniería de requisitos
  - IEEE 830-1998 Prácticas recomendadas para la especificación de requisitos de software
  - IEEE 1233-1998 Guía para desarrollar especificaciones de requisitos de sistema
  - NC ISO/IEC 25010:2016 Ingeniería de software y sistemas – Requisitos de la calidad y evaluación de software (square) – Modelos de la calidad de software y sistemas

Laboratorio

- Lab 1 Comente en clase “**la Política de Seguridad de su Organización**”
  - Cual es la política de seguridad de su organización? Que entiende Ud.?
  - Según la norma ISO 27001, Identifique 5 activos de información y su propietario.
  - Realice un análisis de riesgos de los activos de información.

Referencias

- https://www.techrepublic.com/article/popular-mobile-banking-apps-are-riddled-with-security-flaws-and-android-users-are-more-at-risk/
- http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992018000500015&lng=pt&nrm=iso&tlng=pt
- https://www2.deloitte.com/es/es/pages/risk/articles/los-cinco-mayores-ciberataques-de-la-historia.html