UNA REVISIÓN DE LAS BUENAS PRÁCTICAS PARA EL DESARROLLO SEGURO DE APLICACIONES BASADO EN OWASP

Information Systems Security Association – ISSA Chile

http://www.issachile.cl

Universidad San Sebastian

http://www.uss.cl

Fecha: Martes 09 de Agosto de 2016 a las 19:00 hrs.
Lugar: Universidad San Sebastian Sala A304, Facultad de Ingeniería y Tecnología Bellavista 7, Recoleta, Santiago.

Agenda

Palabras de apertura,

Dr. Hernán Villanueva A., Profesor USS.

Bienvenida ISSA Chile

Sr. Juan Anabalón, Presidente ISSA Chile.

Charla: Buenas Prácticas de Desarrollo Seguro de Aplicaciones

Resumen

Las prácticas inseguras de desarrollo web repercuten en vulnerabilidades que son costosas de solucionar en el software y conllevan muchas veces al robo de datos sensibles.

Debido a esto, los desarrolladores hoy en día deben garantizar que las prácticas de desarrollo seguro, como la formalización de requerimientos de seguridad y revisiones, se incorporan en cada fase del ciclo de vida del desarrollo de software para que las aplicaciones sean diseñadas, codificadas e implementadas con los requisitos de seguridad adecuados, deben integrarse las buenas prácticas en las operaciones del día con un enfoque puesto en los riesgos de seguridad en los procesos de negocio. Todo esto independientemente del dispositivo que se utiliza para la programación.

Esta charla se presentará un conjunto mínimo de prácticas de codificación segura que deben ser implementadas durante el desarrollo y despliegue de aplicaciones para asegurar los componentes principales de acuerdo a la metodología de desarrollo adoptada, que podría ser modelo de cascada tradicional, ágil o cualquier otro. Se presenta los casos de falla más comunes según Open Web Application Security Project (OWASP) y como se debe solucionar los problemas encontrados.

Expositor:

Gustavo Nieves Arreaza. Es Ingeniero de sistemas de la Universidad Santa María y diplomado en Cisco CCNA Universidad Fermín Toro. Venezuela. Gustavo tiene conocimiento profundo de las vulnerabilidades de aplicaciones web comunes (XSS, CSRF, clickjacking) y sus estrategias de mitigación; habilidades solidas de desarrollo Javascript / CoffeeScript, shell scripting e idiomas Estáticos C #, VB, C++,Java; conocimiento de las vulnerabilidades de Seguridad de Sistemas y Técnicas de remediación.