CYBER 2019SEC

SAFECON

Academia de Programación Segura

owasp based

ÍNDICE

1. WORKSHOP CODIFICACION OWASP TOP10

1.1. Antecedentes

La ciberseguridad es un factor que impacta comercialmente a clientes y proveedores, las organizaciones necesitan proteger los datos y la información de sus negocios de forma preventiva y evidenciar ante el mercado que se preocupan seriamente de la seguridad.

Un aspecto complejo es crear aplicaciones de software que sean robustas y seguras. Esta capacidad de resiliencia y cumplimiento de altos niveles de ciberseguridad en el ciclo de vida del desarrollo del software, requiere esfuerzo, inversión y perseverancia.

El punto de partida que la industria definio hace varios años es OWASP TOP10 [1], un estándar de facto, que identifica los diez mayores riesgos de seguridad que deben ser mitigados, al construir aplicaciones.

En este workshop de “Desarrollo Seguro” se entrenará durante todo un día, usando como referencia la versión de OWASP TOP10:2017, aplicado a la construcción del software en un tipico SDLC[2], con ejercitación en laboratorios prácticos.

Los contenidos específicos del workshop que se impartirá en CybersecChile 2019, son extraidos desde los primeros niveles del **“SAFECON: DevCertification Roadmap”** (msrcados en fondo amarillo) y concentran los conocimientos necesarios para entender el **ciclo de vida del desarrollo seguro de software** y aplicar OWASP TOP10 en la fase de programación de software.

Todos los contenidos que SAFECON[3] utiliza en su malla de certificación se basan en buenas prácticas y modelos validados por la industria TI. Los niveles actuales para “Desarrollon Seguro” conducente a certificación son:

Contenidos entrenados por Nivel	Nivel 1 Foundations	Nivel 2 Avanced	Nivel 3 Certificated
SDLC: Ciclo de Vida del Software	✧	✧	✧
Exigencias internacionales y normativas PCI-DSS, ISO27001	✧	✧	✧
Requisitos de Seguridad		✧	✧
Planificación y Riesgos	✧	✧	✧
Diseño y Modelos de Amenazas			✧
Owasp Top10, codificación segura	✧	✧	✧
Testing de Seguridad		✧	✧
Liberación y hardening			✧
Criptografía aplicada		✧	✧
Explotación de vulnerabilidades			✧
Examen escrito del aprendizaje logrado	✧	✧	✧
Preparación al examen de certificación Internacional			✧

1.2. Objetivos

Conocer y entender los diez riesgos de OWASP TOP10:2017, las amenazas que son las más comunes y vigentes para aplicaciones web.

Comprender las técnicas de programación segura y como se interrelacionan entre las fases del ciclo de vida para desarrollar software seguro.

Ejercitar de manera práctica con ejercicios seleccionados desde “Hands-On laboratory” oficiales del roadmap de entrenamiento, algunos de los casos más recurrentes de riesgo de OWASP TOP10:2017.

Finalmente, conocer los pasos siguientes que debería cumplir un profesional que desee lograr la certificación internacional, en programación segura.

1.3. Audiencia

Este curso es adecuado para personal con experiencia en la creación de aplicaciones y servicios web desde el punto de vista de la ingeniería de software, y para los colaboradores que quieren convertirse en auditores y/o ingenieros de seguridad de aplicaciones / analistas / testeadores, y todo individuo involucrado en actividades del tipo desarrollo, testing, administración o versionamiento de aplicaciones.

1.4. Contenidos

A continuación se indican las actividades y los contenidos que están alineados con los referentes de industria: OWASP TOP10, PCI-DSS y los requisitos para construir aplicaciones seguras exigidas por la industria de pagos electrónicos.

- Lección 1: Comprender la seguridad de la información, las amenazas y la taxonomía actual de los ciberataques a las aplicaciones
- Lección 2: Recopilación de Requisitos de Seguridad
- Lección 3: Arquitectura y Diseño de Aplicaciones Seguras
- Lección 4: Prácticas de Codificación Segura, para mitigar OWASP TOP10:2017
    - L4.1 (A1:2017) Inyección
    - L4.2 (A2:2017) Pérdida de Autenticación
    - L4.3 (A3:2017) Exposición de Datos Sensibles
    - L4.4 (A4:2017) Entidades Externas XML (XXE)
    - L4.5 (A5:2017) Pérdida de Control de Acceso
    - L4.6 (A6:2017) Configuración de Seguridad Incorrecta
    - L4.7 (A7:2017) Cross-Site Scripting (XSS)
    - L4.8 (A8:2017) Deserialización Insegura
    - L4.9 (A9:2017) Uso de Componentes con Vulnerabilidades Conocidas
    - L4.10 (A10:2017) Registro y Monitoreo Insuficientes

Evaluación: El nivel de aprendizaje final se mide con un examen escrito.

1.5. Contenidos detallados del training

El detalle de cada contenido es

- Lección 1: Comprender la seguridad de la información, las amenazas y la taxonomía actual de los ciberataques a las aplicaciones
    - Introducción a la Seguridad de la Información
    - Estadística de riesgos y ciberataques en latam
    - Defensa en profundidad (estrategia del castillo)
    - Defensa en el Ciclo de Vida del Software (SDLC)

- Lección 2: Recopilación de Requisitos de Seguridad
    - Ingeniería de Requisitos
    - Ambigüedad y errores comunes
    - Trazabilidad de Requisitos
    - Análisis del impacto y Gestión de Cambios
    - Buenas prácticas para Requisitos de Seguridad del Software

- Lección 3: Arquitectura y Diseño de Aplicaciones Seguras
    - Modelos de Desarrollo
    - Uso de Frameworks y librerias
    - Exposición y riesgo para vulnerabilidades conocidas
    - Seguridad por capas
    - Modelamiento de amenazas

- Lección 4: Prácticas de Codificación Segura, para mitigar OWASP TOP10:2017
    - L4.1 (A1:2017) Inyección
    - L4.2 (A2:2017) Pérdida de Autenticación
    - L4.3 (A3:2017) Exposición de Datos Sensibles
    - L4.4 (A4:2017) Entidades Externas XML (XXE)
    - L4.5 (A5:2017) Pérdida de Control de Acceso
    - L4.6 (A6:2017) Configuración de Seguridad Incorrecta
    - L4.7 (A7:2017) Cross-Site Scripting (XSS)
    - L4.8 (A8:2017) Deserialización Insegura
    - L4.9 (A9:2017) Uso de Componentes con Vulnerabilidades Conocidas
    - L4.10 (A10:2017) Registro y Monitoreo Insuficientes

1.6. Relatores SAFECON

Carlos Allendes ,
Presidente Owasp Chile

linkedin

Presidente del capítulo chileno de www.OWASP.cl, co-fundador de los capítulos de Owasp en Puerto Rico, Honduras y República Dominicana. Charlista y organizador de eventos para Desarrollo Seguro, QA y ciberseguridad de aplicaciones.

Ingeniero Civil en Informática de la Universidad de Santiago de Chile. Consultor internacional en proyectos gubernamentales y privados, para acreditación PCI-DSS, evaluación CMMi, implementación de procesos ITIL, ISO.27001 y PMO en retail, banca y telco.

Empresario y socio en www.QualityFactory.cl, Investigador y docente en Desarrollo Seguro, ciberseguridad y mejoramiento de procesos.

Oscar Orellana,
Owasp Iquique

linkedin

Lider de OWASP Iquique, relator y docente, Además es fundador de la consultora OCOA Cybersecurity

Especialista ISO-27001 y Seguridad de la Información es Master en Ciberseguridad © de IMF Business School, ha gestionado diversos tipos de proyectos para seguridad física, televigilancia y seguridad perimetral, como implementador de Arquitectura tecnológica y procesos. Es relator habitual en congresos de ciberseguridad sobre ISO 27001, Seguridad Física, Convenio de Budapest, proyecto de Ley de Ciberseguridad Chile

Consultor, investigador y docente en Desarrollo Seguro y mejoramiento continuo de procesos.

Javier Pinochet,
Owasp Arica

linkedin

Lider de OWASP Arica, relator y docente, Además es fundador y gerente general de la consultora www.pentesters.cl

Especialista en hacking Ético, es Ingeniero Informático y Consultor en Ciberseguridad, Seguridad en Aplicaciones y Pruebas de Penetración y Análisis de Vulnerabilidades Web.

Tiene experiencia Laboral en el Área de Telecomunicaciones e IT por mas de 15 años y se desarrolla como docente y conferencista en ciberseguridad.

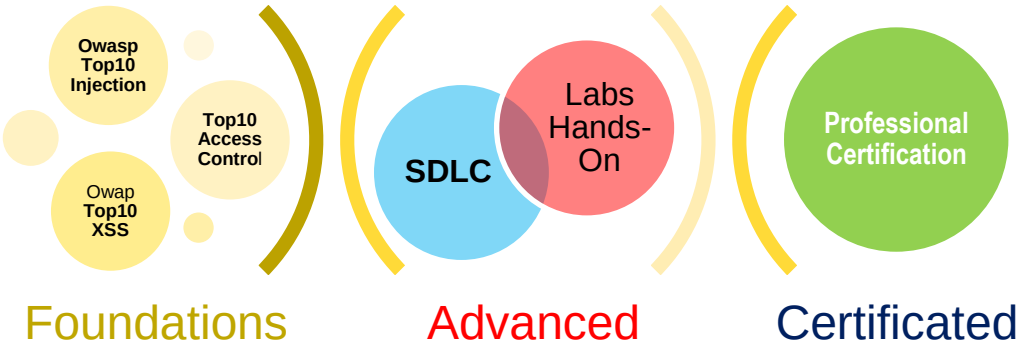
2. REFERENCIAS

[1]. **OWASP TOP10**, Ranking de los diez riesgos más críticos en Aplicaciones Web https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[2]. **SDLC** Ciclo de Vida del Desarrollo de Software (SDLC por las siglas en inglés: **S**oftware **D**evelopment **Life C**ycle

[3]. **SAFECON**, asociación de voluntarios que coordina las actividades de divulgación y formación basadas en material oficial de OWASP.

Academy: Trainings & Certification Roadmap



- Nivel 1: Foundations Training. Con workshops de nivelación de conceptos y normas internacionales. Entender y mitigar de los 10 riesgos descritos en Owasp Top10 versión 2017, describe cada riesgo, su forma de ataque y la remediación propuesta por Owasp. La duración del curso es de 7 horas.

- Nivel 2: Advanced Training. Es un entrenamiento de 14 horas con laboratorios de programación segura para un lenguaje a elección (.NET, JAVA o PHP) y sus Bases de Datos (se recomienda abordar un solo lenguaje y aplicarlo al modo real que usa la organización).

- Nivel 3: Certification Training. Entrenamiento de 24 horas. Está centrado en el proceso completo de creación del software y los controles de ciberseguridad aplicados. Prepara al estudiante para rendir el examen de certificación con validez internacional (no incluye el voucher del examen)

Contenidos entrenados por Nivel	Nivel 1 Foundations	Nivel 2 Avanced	Nivel 3 Certificated
SDLC: Ciclo de Vida del Software	✧	✧	✧
Exigencias internacionales y normativas PCI-DSS, ISO27001	✧	✧	✧
Requisitos de Seguridad		✧	✧
Planificación y Riesgos	✧	✧	✧
Diseño y Modelos de Amenazas			✧
Owasp Top10, codificación segura	✧	✧	✧
Testing de Seguridad		✧	✧
Liberación y hardening			✧
Criptografía aplicada		✧	✧
Explotación de vulnerabilidades			✧
Examen escrito del aprendizaje logrado	✧	✧	✧
Preparación al examen de certificación Internacional			✧