Learning Think

Education One Experience

by

TWS²

Technology as a Service

Taller online de: OWASP TOP 10, OWASP API + Desarrollo Seguro

1. Entendimiento y Enfoque de la Capacitación

Antecedentes

Learning Think
Education One Experience

OWASP (Open Web Application Security Project) es una metodología de seguridad de código abierto y colaborativa que se utiliza como referente para auditorias de seguridad de aplicaciones web.

Los Toolkits de OWASP Enterprise Security API ayudan a los desarrolladores de software a protegerse de problemas de seguridad relacionados con el diseño o implementación de una aplicación. Es una Colección de clases que encapsulan los controles de seguridad mas importantes para una aplicación.

2. Contenido y Audiencia

Contenido:

Learning Think
Education One Experience

- Conceptos básicos de seguridad informática.
- ¿Qué es una vulnerabilidad?
- Set de herramientas básicas y la guía de configuración de las mismas (BurpSuite Community, Zap Proxy, etc).
- OWASP Top 10 -2017
  - A1:2017-Injection
  - A2:2017-Broken Authentication
  - A3:2017-Sensitive Data Exposure
  - A4:2017-XML External Entities (XXE)
  - A5:2017-Broken Access Control
  - A6:2017-Security Misconfiguration
  - A7:2017-Cross-Site Scripting (XSS)
  - A8:2017-Insecure Deserialization
  - A9:2017-Using Components with Known Vulnerabilities
  - A10:2017-Insufficient Logging & Monitoring
- OWASP Security API
  - API1:2019 Broken Object Level Authorization
  - API2:2019 Broken User Authentication
  - API3:2019 Excessive Data Exposure
  - API4:2019 Lack of Resources & Rate Limiting
  - API5:2019 Broken Function Level Authorization
  - API6:2019 Mass Assignment
  - API7:2019 Security Misconfiguration
  - API8:2019 Injection
  - API9:2019 Improper Assets Management
  - API10:2019 Insufficient Logging & Monitoring
- Cuenta con 50 ejercicios prácticos destinados a entender y cubrir de

  OWASP Top 10 -2017- y OWASP Security API durante el transcurso del curso.
- Examen final con 10 preguntas multiple choice, más 10 ejercicios

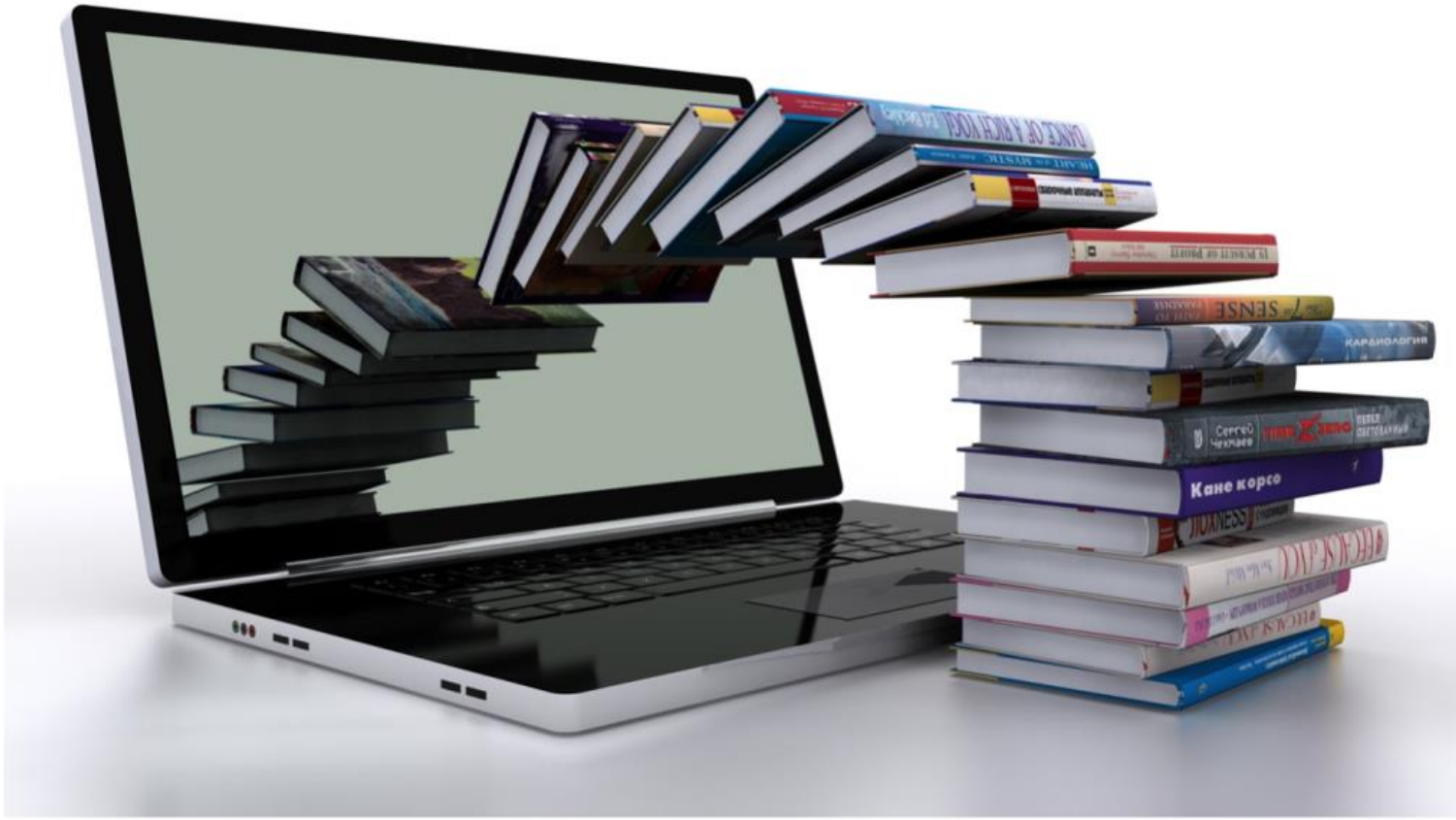
  prácticos relacionados a los temas vistos.

Audiencia

Learning Think
Education One Experience

- Esta capacitación es para consultores de seguridad, desarrolladores o cualquier persona interesada en aprender seguridad de las aplicaciones Web y su API/Backend.
- Los ejercicios son graduales, con dificultad básica, intermedia y avanzada para cada una de las temáticas.

3. Objetivos y Logística



Requerimientos previos del estudiante

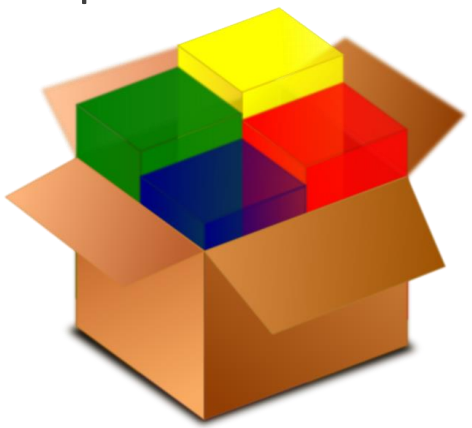
Learning Think
Education One Experience

- Habilidades básicas de Linux.
- Mínimo de experiencia analizando/leyendo código.
- La capacitación cubre temas que van de forma gradual, con temas introductorios y teóricos, con configuración de algunas herramientas asociadas al análisis de vulnerabilidades.
- Computadora con mínimo 8GB de RAM y 80GB disco disponible (preferentemente disco de estado sólido).
- VMware/Virtualbox con Kali Linux, docker instalado.
- Acceso a algunas plataformas complementarias que se darán durante la coordinación del curso (TryHackme, PentesterLab, etc).

Entregables

Learning Think
Education One Experience

- Diapositivas para el seguimiento de las clases.
- VM personalizada para pentesting práctico y con los ejercios para ser ejecutados también localmente.
- Creación de usuarios dentro de las instancias de AWS, y asignación de puertos, para poder resolver los mismos de manera remota.
- Más de 50 ejercicios prácticos.
- Una lista extensa de buenas lecturas (“good practices”) y artículos para
- aprender la seguridad de las aplicaciones Web y su API.
- Certificado de finalización satisfactoria.
- Canal de Slack para mejorar la comunicación con los alumnos, durante el transcurso de la capacitación.
- Grabación de aquellos ejercicios en donde los alumnos tengan dudas durante la resolución de los mismos.



Costos y Logística del Curso

Learning Think
Education One Experience

ÍTEM	DETALLE
Valor	USD $699 por asistente. Público en General USD $599 por asistente*. (Precios no incluye IVA) *Precio exclusivo para cliente de Dycotein y Socios del CIISCA
Lugar y Fecha:	Curso en modalidad Online con tutor en vivo. Fechas de inicio 15 de Mayo
Carga Horaria:	22 horas dividido en 8 jornadas de dos horas y media por día
Horario:	De 18H30 a 21H00 entre semana

Condiciones

- **Se necesitan 6 asistentes para abrir el curso**
- **Forma de pago 50% por anticipado 50% una vez terminado el servicio.**

3. Facilitadores

Trainer

Juan Urbano, Ingeniero de nacionalidad argentina, trabajó para ESET Latinoamérica. Es un consultor de Seguridad Informática con más de 10 años de experiencia. Actualmente especializado en aplicaciones móviles desde hace más de 5 años. Habiendo asistido concurrentemente a capacitaciones como pueden ser Blackhat 2019, Blackhat 2017. Actualmente coordinador del Ekoparty Mobile Hacking Space

Ha realizado también diversas investigaciones, workshops y brindó charlas asociadas al análisis de aplicaciones móviles (OWASP Buenos Aires, OWASP Patagonia, OWASP Cordoba, Ekoparty University Talks, etc).

Contactos:

Ing. Juan Pablo Amón S.

Email: gerencia@tws2.io

WhatsApp +593 995 567 772

Learning Think

Education One Experience

by TWS²

Technology as a Service

Global Trust Association®

ACCREDITED TRAINING & EXAMINATION PROVIDER

CertiProf® | Partner

Agile Alliance®

CORPORATE MEMBER

www.learningthink.io