Curso OWASP API Security Top 10

2	6	En vivo, Virtual, o Personalizado
Sesiones	Horas	

Alonso Eduardo Caballero Quezada

Tengo más de veintidós años de experiencia, y desde hace dieciocho años realizo capacitaciones y consultorías en Hacking, Forense, OSINT, CiberSeguridad, y GNU/Linux

Redes Sociales

LinkedIn

X (Twitter)

YouTube

Facebook

Sitio Web

e-mail

WhatsApp

Presentación

Este proyecto está diseñado para abordar el creciente número de organizaciones los cuales implementan API potencialmente sensibles como parte de sus ofertas de software. Estas API se utilizan para tareas internas y para interactuar con terceros. Desafortunadamente muchas API no se someten a las rigurosas pruebas de ciberseguridad necesarias para protegerlas contra ataques.

El Proyecto de Seguridad de API de OWASP busca aportar valor a los desarrolladores de software y profesionales quienes evalúan la ciberseguridad, destacando los riesgos potenciales de las API inseguras e ilustrando como mitigarlos. Para lograr este objetivo el Proyecto de Seguridad de API de OWASP crea y mantiene un documento con los diez principales riesgos de ciberseguridad de las API, así como un portal de documentación con las mejores prácticas para la creación y evaluación de API.

Muchos desarrolladores y consultores en ciberseguridad de la información se han encontrado con API en sus proyectos. Si bien existen algunos recursos para ayudar a crear y evaluar estos proyectos (como la Guía Rápida para Ciberseguridad REST de OWASP), hasta ahora no existía un proyecto de ciberseguridad integral diseñado para ayudar a desarrolladores, analistas, y defensores de la comunidad.

Este proyecto tiene como objetivos:

Crear el documento OWASP Top Ten API Security Risks, el cual permite destacar fácilmente los riesgos más comunes en este ámbito.

Crear un portal de documentación para los desarrolladores creen API de manera segura.

Colaborar estrechamente con la comunidad de ciberseguridad para mantener una documentación actualizada la cual evolucione al ritmo de las tendencias de ciber seguridad.

Alonso Eduardo
Caballero Quezada
(ReYDeS)

Curso OWASP API Security Top 10

Temario

Prefacio
Introducción
Notas de Publicación
Riesgos de Seguridad en API
Diferencias entre 2019 y 2023
API1:2023 Broken Object Level Authorization (Autorización a nivel de objeto defectuosa)
API2:2023 Broken Authentication (Autenticación defectuosa)
API3:2023 Broken Object Property Level Authorization (Autorización de nivel de propiedad de objeto defectuosa)
API4:2023 Unrestricted Resource Consumption (Consumo de recursos sin restricciones)
API5:2023 Broken Function Level Authorization (Autorización de nivel de función defectuosa)
API6:2023 Unrestricted Access to Sensitive Business Flows (Acceso sin restricciones a flujos de negocio sensibles)
API7:2023 Server Side Request Forgery (Falsificación de solicitudes del lado del servidor)
API8:2023 Security Misconfiguration (Mala configuración de seguridad)
API9:2023 Improper Inventory Management (Gestión inadecuada de inventarios)
API10:2023 Unsafe Consumption of APIs (Consumo inseguro de API)
¿Qué Sigue para los Desarrolladores?
¿Qué Sigue para DevSecOps?

Beneficios

- Acceso al aula virtual por 60 días
- Acceso a las sesiones en vivo
- Video de las dos (2) sesiones
- Acceso libre a las sesiones en vivo de los siguientes cursos a dictarse
- Material utilizado durante el desarrollo del curso
- Dos (2) horas de asesoría personalizada en vivo por videoconferencia
- Libro "Fundamentos de Hacking Web" escrito por el instructor
- Certificado digital de participación
- Certificado digital de aprobación por una duración total de 16 horas

Inversión

Perú: S/. 225 Soles

- Depósito o transferencia interbancaria a Scotiabank
- Pago mediante YAPE o PLIN

Otros países: $ 70 Dólares

- Pago mediante PayPal

Escriba un mensaje al WhatsApp https://wa.me/51949304030 para proporcionarle los datos pertinentes.

Información

Para obtener más información sobre este curso tiene a su disposición los siguientes mecanismos de contacto.

WhatsApp: https://wa.me/51949304030

Correo electrónico: reydes@gmail.com