# *API REST, diseño, arquitectura y seguridad*

*Curso práctico de 3 días - 21h*
*Ref.: REH - Precio 2024: 1 440€ sin IVA*

Los servicios web conformes al estilo de arquitectura REST establecen la interoperabilidad entre ordenadores en Internet. Aprenderá las buenas prácticas de diseño y desarrollo y las herramientas asociadas, así como las vulnerabilidades más comunes y las mejores formas de protegerse contra ellas.

### OBJETIVOS PEDAGÓGICOS

Al término de la formación, el alumno podrá:

Familiarícese con las herramientas que le ayudarán desde el diseño hasta la implantación y supervisión de sus API.

Comprender las amenazas a sus API

Identificar las vulnerabilidades más comunes

Identifique los puntos débiles de una API y protéjala

Dominio de las mejores prácticas en el diseño, desarrollo y arquitectura de las API ReST

## PROGRAMA

última actualización: 08/2024

### 1) Introducción a las API ReST

- Arquitecturas, aplicaciones y API de n niveles.
- Las principales diferencias entre una API REST y una API SOA.
- H.A.T.E.O.A.S. Gestión de recursos y enlaces hipermedia.

*Trabajo práctico : Diseño de una API flexible, escalable, resistente y de alto rendimiento.*

### 2) Buenas prácticas

- Convenciones y buenas prácticas.
- Técnicas y estrategias de control de versiones.
- Buenos planteamientos de diseño y desarrollo.

*Trabajo práctico : Definición y diseño de una API ReST.*

### 3) La caja de herramientas

- Diseño de API ReST con OpenAPI y Swagger.
- Uso de Cartero o Insomnio.
- Entorno y herramientas de prueba (generador JSON, servidor JSON).
- Simulacro de API.

*Trabajo práctico : Especificación de una API ReST con Swagger. Implementar y probar una API ReST.*

### 4) Recordatorio de seguridad

- Principios fundamentales de la seguridad informática. Amenazas e impacto potencial.
- APIs específicas: Farming y Throttling.
- BFA e IA: las nuevas amenazas.
- Las distintas inyecciones (XSS, BSI, XSRF, RFI, XPi, etc.).
- Exposición de datos sensibles. Protección del acceso.
- Deserialización insegura. Componentes vulnerables.
- Registro y supervisión.

### PARTICIPANTES

Desarrolladores web front-end y back-end, arquitectos.

### REQUISITOS PREVIOS

Conocimientos de HTTP y desarrollo web: JavaScript/HTML.

### COMPETENCIAS DEL FORMADOR

Los expertos que imparten la formación son especialistas en las materias tratadas. Han sido validados por nuestros equipos pedagógicos, tanto en el plano de los conocimientos profesionales como en el de la pedagogía, para cada curso que imparten. Cuentan al menos con entre cinco y diez años de experiencia en su área y ocupan o han ocupado puestos de responsabilidad en empresas.

### MODALIDADES DE EVALUACIÓN

El formador evalúa los progresos pedagógicos del participante a lo largo de toda la formación mediante preguntas de opción múltiple, escenificaciones de situaciones, trabajos prácticos, etc.
El participante también completará una prueba de posicionamiento previo y posterior para validar las competencias adquiridas.

### MEDIOS PEDAGÓGICOS Y TÉCNICOS

• Los medios pedagógicos y los métodos de enseñanza utilizados son principalmente: ayudas audiovisuales, documentación y soporte de cursos, ejercicios prácticos de aplicación y ejercicios corregidos para los cursillos prácticos, estudios de casos o presentación de casos reales para los seminarios de formación.
• Al final de cada cursillo o seminario, ORSYS facilita a los participantes un cuestionario de evaluación del curso que analizarán luego nuestros equipos pedagógicos.
• Al final de la formación se entrega una hoja de presencia por cada media jornada de presencia, así como un certificado de fin de formación si el alumno ha asistido a la totalidad de la sesión.

### MODALIDADES Y PLAZOS DE ACCESO

La inscripción debe estar finalizada 24 horas antes del inicio de la formación.

### ACCESIBILIDAD DE LAS PERSONAS CON DISCAPACIDAD

¿Tiene alguna necesidad específica de accesibilidad? Póngase en contacto con la Sra. FOSSE, interlocutora sobre discapacidad, en la siguiente dirección psh-accueil@orsys.fr para estudiar de la mejor forma posible su solicitud y su viabilidad.

- Presentación del OWASP TOP 10.
- Descubra Pentesting.
- Introducción a Restler-Fuzzer.

*Trabajo práctico : Presentación de una serie de soluciones de seguridad para sitios web.*

### 5) Autenticación y autorización

- Seguridad de autenticación.
- Sistema de registro.
- Seguridad del servidor.
- Canonicalización, evasión y sanitización.
- Gestión de permisos: acceso basado en funciones frente a acceso basado en recursos.
- CORS (Cross-Origin Resource Sharing) y CSRF (Cross-Site Request Forgery).
- Autenticación con OAuth2 y OpenID Connect: vocabulario y flujo de trabajo.

*Trabajo práctico : Buscar y explotar vulnerabilidades de autenticación y autorización.*

### 6) Middleware y JWT (JSON Web Token)

- Un recordatorio de la criptografía.
- Los principios fundamentales de JWT.
- Riesgos intrínsecos y vulnerabilidades.

*Trabajo práctico : Desafío en una API no segura.*

### 7) Pruebas API

- Las 10 áreas de las pruebas API.
- Ventajas y limitaciones de las pruebas API únicas.
- Creación de una API comprobable por diseño.
- Pruebas de endurecimiento.
- Requisitos de las pruebas de conformidad API.
- Prácticas probadas para reducir los costes de las pruebas.

*Trabajo práctico : Pruebas de una API con Postman, creación de un escenario de pruebas basado en datos e integración de CLI en Newman.*

### 8) Gestión de API

- Ventajas de las soluciones de gestión de API.
- Gravitee: una API de código abierto moderna y eficaz.
- Gestión del acceso a las API, Diseño de las API, Gestión de las API, Despliegue de las API y Observabilidad de las API.

*Trabajo práctico : Utilice una solución de gestión de API para desplegar una API.*

## FECHAS

Contacto