

Course : REST API, design, architecture and security

Practical course - 3d - 21h00 - Ref. REH

Price : 2220 CHF E.T.

★★★★☆ 4,3 / 5

BEST

Les services web conformes au style d'architecture REST établissent une interopérabilité entre les ordinateurs sur Internet. Vous pourrez découvrir les bonnes pratiques de conception, de développement, les outils associés ainsi que les vulnérabilités les plus communes et les meilleurs moyens de s'en prémunir.

Teaching objectives

At the end of the training, the participant will be able to:

- ✓ Get to grips with the tools that will support you from design to deployment and supervision of your APIs
- ✓ Understand the threats to your APIs
- ✓ Identify the most common vulnerabilities
- ✓ Identify API weaknesses and protect them
- ✓ Master best practices in ReST API design, development and architecture

Intended audience

Front-end and back-end web developers, architects.

Prerequisites

Connaissances HTTP ainsi que des connaissances en développement web : JavaScript/HTML.

Course schedule

1 Introduction to ReST APIs

- n-tier architectures, applications and APIs.
- The essential differences between a REST API and a SOA API.
- H.A.T.E.O.A.S. Resource management and hypermedia links.

Hands-on work

Design of a flexible, scalable, resilient and high-performance API.

PARTICIPANTS

Front-end and back-end web developers, architects.

PREREQUISITES

Connaissances HTTP ainsi que des connaissances en développement web : JavaScript/HTML.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more. Participants also complete a placement test before and after the course to measure the skills they've developed.

2 Best practices

- Conventions and best practices.
- Versioning Techniques and Strategies.
- Good design and development approaches.

Hands-on work

Definition and design of a ReST API.

3 The toolbox

- API Mock.
- Designing ReST APIs with OpenAPI and Swagger.
- Use of Postman or Insomnia.
- Test environment and tools (JSON Generator. JSON Server).

Hands-on work

Specifying a ReST API with Swagger. Implement and test a ReST API.

4 Safety reminder

- The main principles of IT security. Threats and potential impacts.
- Specific APIs: Farming and Throttling.
- BFA and AI: the new threats.
- Various injections (XSS, BSI, XSRF, RFI, XPI, etc.).
- Exposure of sensitive data. Secure access.
- Insecure deserialization. Vulnerable components.
- Logging and monitoring.
- Presentation of the OWASP TOP 10.
- Discover Pentesting.
- Introduction to Restler-Fuzzer.

Hands-on work

Presentation of a few website security solutions.

5 Authentication and authorization

- Authentication security.
- Logging system.
- Server-side security.
- CORS (Cross-Origin Resource Sharing) and CSRF (Cross-Site Request Forgery).
- Canonicalization, Escaping and Sanitization.
- Permission management: Role-Based Access vs. Resource-based access.
- Authentication with OAuth2 and OpenID Connect: vocabulary and workflow.

Hands-on work

Search for and exploit authentication and authorization vulnerabilities.

TEACHING AIDS AND TECHNICAL RESOURCES

- The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
- At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
- A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

6 Middleware and JWT (JSON Web Token)

- A reminder of cryptography.
- The main principles of JWT.
- Intrinsic risks and vulnerabilities.

Hands-on work

Challenge on an unsecured API.

7 API testing

- The 10 areas of API testing.
- Advantages and limitations of one-shot API testing.
- Build an API that's testable by design.
- Hardening tests.
- API compliance testing requirements.
- Proven practices for reducing testing costs.

Hands-on work

API testing with Postman, creation of a Data Driven test case, and CLI integration in Newman.

8 API Management

- The benefits of API Management solutions.
- Gravitee: modern, efficient opensource APIm.
- API Access Management, API Design, API Management, API Deployment and API Observability.

Hands-on work

Use an API Management solution to deploy an API.

Dates and locations

REMOTE CLASS

2026 : 1 June, 27 July, 7 Oct., 25 Nov.