AMBIENT-IT

+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 19/03/2024

Sign up

Angular application security training

2 days (14 hours)

We are Angular 13, 12, 11, 10, 9, 8, 7 & 6 Ready!

Presentation

The Angular framework has revolutionized the world of Web applications, bringing a number of technical building blocks and new concepts to make life easier for developers.

In this context, traditional security approaches have outlived their usefulness, and need to be adapted to the particularities of this framework in order to cope with the new risks and threats it faces.

The aim of this training course is to provide you with the knowledge and best practices you need to build secure Angular applications by design.

With a mix of theory, demos, quizzes and several labs, participants in this course will have the opportunity to manipulate techniques and concepts to secure their Angular applications, through the following themes:

- Angular's native security mechanisms
- Browser-side security mechanisms, and how to test/implement them in Angular ;
- Common mistakes to avoid when protecting an Angular-based SPA
- The security of browser storage mechanisms
- Best practices for implementing OAuth 2.0 and OIDC

Like all our training courses, this one will introduce you to the latest stable version and its new features: Angular 14 and Redux 5.

Objectives

- Master the basics of application security

- Know how to implement Content Security Policy (CSP)
- How to protect yourself against malicious code injections
- Master the secure architecture of front-end applications
- Discover the advanced security techniques of OAuth 2.0

Target audience

- Developers
- Technical architects
- Project managers
- Directors

Prerequisites

Fundamental knowledge of Angular, or have completed our Angular training course

Angular application security training program

Introduction

- General information on front-end application security: risks and threats
- UI rectification attacks: how do they work?
- Leakage of sensitive information in internal browser storage
- Configuring security headers for browsers

Javascript malicious code injections

- Introduction to Cross-Site Scripting (XSS) vulnerabilities
- XSS defense mechanisms in Angular
- XSS traps in Angular
- XSS and server-side rendering
- Using the Trusted Types mechanism with Angular

Implementing Content Security Policy (CSP)

- Introduction to the Content Security Policy (CSP) mechanism
- Common mistakes in CSP policies
- CSP deployment for Angular
- Best practices on CSP

Advanced security mechanisms for front-end applications

- Secure your front-end application with the Subresource Integrity (SRI) mechanism
- Sandboxing do conteny non-fiable
- Sandboxing strategies in HTML5

Secure architecture for front-end applications

- Patterns and best practices for a secure architecture
- Securing the browser's local storage mechanisms
- Using the Crypto Web API

OAuth 2.0 advanced security

- Attacks and risks targeting OAuth 2.0 security in the context of SPAs
- Best practices for implementing OAuth 2.0 and OpenID Connect for SPAs and Single Sign-On
- Introduction to the Backend-For-Frontend pattern
- Security recommendations for OAuth 2.0 in Angular
- What's new in OAuth 2.1?

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.