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

Mis à jour le 21/11/2024

S'inscrire

Formation Sécurité des applications Angular

2 jours (14 heures)

Nous sommes Angular 13, 12, 11, 10, 9, 8, 7 & 6 Ready !

Présentation

Le framework Angular a révolutionné le monde des applications Web en apportant plusieurs briques techniques et nouveaux concepts pour faciliter la vie aux développeurs.

Face à ce contexte, les approches de sécurités traditionnelles ne sont plus d'actualités, et il est ainsi nécessaire de les adapter aux particularités de ce framework pour faire face aux nouveaux risques et menaces auquel doit-en faire face.

C'est ainsi que l'objectif de cette formation est d'apporter les connaissances et les bonnes pratiques permettant de mettre en place des applications Angular sécurisées « by-design ».

Avec un mixte entre théorie, demos, quizzs et plusieurs labs, les participants à cette formation auront l'occasion de manipuler les techniques et concepts permettant de sécuriser leurs applications Angular, et cela, à travers les thèmes suivants :

- Les mécanismes de sécurité natifs dans Angular
- Les mécanismes de sécurité côté browser, et comment les tester/mettre en œuvre dans le cadre des applications Angular ;
- Les erreurs communes à éviter pour protéger une SPA basée sur Angular
- La sécurité des mécanismes de stockage dans le browser
- Les bonnes pratiques de mise en place de l'OAuth 2.0 e OIDC

Comme toutes nos formations, celle-ci vous présentera la dernière version stable en date et ses nouveautés : Angular 19 ainsi que Redux 5.

Objectifs

- Maîtriser les bases de la sécurité des applications

- Savoir mettre en œuvre du Content Security Policy (CSP)
- Savoir se protéger des injections de code malveillant
- Maîtriser l'architecture sécurisée des applications fronts
- Découvrir les techniques de la sécurité avancée de l’OAuth 2.0

Public visé

- Développeurs
- Architectes techniques
- Chefs de projet
- Administrateurs

Pré-requis

Connaissances fondamentales sur Angular, ou avoir effectué notre formation Angular

Programme de notre formation Sécurité des applications Angular

Introduction

- Généralité sur la sécurité des applications front : risques et menaces
- Les attaques « UI redressing » : comment ça fonctionne ?
- Fuite d’information sensible dans le stockage interne des browsers
- Configuration des headers de sécurité pour les browsers

Les injections du code malveillant Javascript

- Introduction sur les failles Cross-Site Scripting (XSS)
- Mécanismes de défense contre les XSS dans Angular
- Les pièges XSS dans Angular
- XSS et server-side rendering
- Utilisation du mécanisme « Trusted Types » avec Angular

Mise en œuvre du Content Security Policy (CSP)

- Introduction au mécanisme de Content Security Policy (CSP)
- Les erreurs communes des politiques CSP
- Déploiement du CSP pour Angular
- Bonnes pratiques sur le CSP

Mécanismes de sécurité avancés pour les applis fronts

- Sécuriser votre application front avec le mécanisme Subresource Integrity (SRI)
- Sandboxing do conteny non-fiable
- Les stratégies de sandboxing dans HTML5

Architecture sécurisée des applications fronts

- Les patterns et bonnes pratiques d'une architecture sécurisée
- Sécurisation des mécanismes de stockage local du browser
- Utilisation de l'API Web Crypto

Sécurité avancée de l'OAuth 2.0

- Attaques et risques ciblant la sécurité de l'OAuth 2.0 dans le contexte des SPAs
- Les bonnes pratiques de mise en œuvre de l'OAuth 2.0 et l'OpenID Connect pour les SPAs et le Single Sign-On
- Introduction au pattern « Backend-For-Frontend »
- Recommandations sur la sécurité de l'OAuth 2.0 dans Angular
- Vue sur les nouveautés de l'OAuth 2.1

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.