

Sécurité applicative : intégrer la sécurité dès la conception (Secure by Design)

2 jours (14 heures)

Expertise

à partir de

1790 € HT par personne (TVA en vigueur)

Contenu mis à jour le 25/09/2026. Document téléchargé le 06/10/2026.

Objectifs

A l'issue de cette formation, vous serez capable de :

- Concevoir une application "Secure by Design"
- Appliquer les bonnes pratiques de sécurité à toutes les phases de développement
- Identifier les principales failles de sécurité applicative et anticiper les menaces
- Décrire le déroulement d'une attaque pour mieux la déjouer.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Développeurs, ops, testeurs, administrateurs, architectes et/ou toute personne concernée par la sécurité des applications au sens large (application Web, site, Web service...).

Prérequis

Pratiquer les langages de développement Web (a minima : HTML, JavaScript, SQL), avoir des connaissances du protocole HTTP et idéalement la connaissance d'un framework front de type Angular, React...

Programme

1 Pendant votre formation

Sécurité applicative : intégrer la sécurité dès la conception (Secure by Design)

Jour 1

Présentation de la démarche de Secure Coding

Secure by Design

- Présentation des 10 principes de sécurité pour concevoir une application sécurisée
- Challenge offensif en équipe pour simuler une attaque applicative

Sécurité du Web : présentation des mécanismes de sécurité des navigateurs Web

- SOP (Same Origin Policy)
- CORS (Cross-Origin Resource Sharing)
- CSP (Content Security Policy)

Revue du top 10 OWASP (Open Web Application Security Project)

Exemples de travaux pratiques (à titre indicatif)

- Mise en pratique des principales attaques avec une application volontairement vulnérable
- Les participants doivent, de manière collaborative, exploiter la faille puis en identifier la cause pour ensuite la corriger
 - Attaque XSS (Cross Site Scripting)
 - Attaque SSTI (Server Side Templating Injection)
 - Attaque REDOS (Regular Expression Denial Of Service)

Jour 2

Exemples de travaux pratiques (à titre indicatif) - Suite

- Mise en pratique des principales attaques (suite du jour 1)
 - Attaque IDOR (Insecure Direct Object Reference)
 - Attaque Mass Assignment
 - Attaque SQL injection
 - Attaque CSRF (Cross Site Request Forgery)

Bonnes pratiques de sécurité

- Mesures de protection contre les "Bot" (Captcha)
- Sécurité des cookies
- Protocole HTTPS : paramètres TLS et entêtes HTTP

Exemple de travaux pratiques (à titre indicatif)

- Mise en pratique au travers d'un atelier de Secure Coding pour définir sa stratégie de sécurité applicative

- Identification d'un plan d'action post formation

Synthèse et partage des retours sur la formation

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* nous consulter pour la faisabilité en distanciel

** ratio variable selon le cours suivi

Accessibilité aux personnes en situation de handicap