

C# – Sécurité applicative avec .NET

3 jours (21 heures)

Expertise

Présentiel ou classe à distance

à partir de

2 205 € HT par personne (TVA en vigueur) Repas inclus en présentiel

Contenu mis à jour le 25/09/2026. Document téléchargé le 04/10/2026.

Réservez la formation en C# – Sécurité applicative avec .NET. La formation est ouverte aux développeurs et auditeurs en sécurité.

Objectifs

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

- Reconnaître les mécanismes de sécurité de .NET
- Expliquer les principales failles de sécurité applicative
- Mettre en oeuvre le Code Access Security et le Role Based Security
- Sécuriser des "Assemblies"
- Authentifier et autoriser l'accès aux applications ASP.NET
- Chiffrer des données avec le Framework .NET
- Créer des tests visant à éprouver la sécurité des applications
- Formuler des exigences de sécurité aux autres corps de métiers.

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

À qui s'adresse cette formation ?

Pentesters et développeurs.

Prérequis

Avoir des connaissances en développement d'application en langage .NET ou langage assimilé.

Programme

1 Pendant votre formation

C# – Sécurité applicative avec .NET

Jour 1 – Matin

Rappels sur la sécurité applicative

- Fonctionnement de la pile d'exécution
- L'analyse de code statique et dynamique
- Le principe du moindre privilège
- L'hijacking de ressources
- Les overflows
- Les protections lors de l'exécution
- Le chiffrement des données au repos et en transit

Sécurité du Framework .NET

- La revue de code
- La validation des entrées
- Les "namespaces"
- Le sandboxing
- La gestion sécurisée des erreurs

Exemples de travaux pratiques (à titre indicatif)

- Créer une classe de filtrage des entrées utilisateur pour un identifiant, un ID et un email
- Ajouter à ce script une gestion sécurisée des erreurs

Jour 1 – Après-midi

Chiffrement avec C#

- Rappel des bases du chiffrement
- Les fonctions de Hash
- Les algorithmes symétriques type AES
- Les algorithmes asymétriques RSA
- Windows Data Protection et File.Encrypt

- Générer des clés
- Générer des certificats

Exemple de travaux pratiques (à titre indicatif)

- *Créer une classe de chiffrement symétrique et Hash de la donnée chiffrée*

Jour 2 – Matin

L'authentification

- Exploitation d'HTTP basic
- La classe FormsAuthenticationModule
- Le protocole IWA (Integrated Windows Authentication)
- La méthode Application_AuthenticateRequest
- Le contrôle des rôles et permissions
- La classe UrlAuthorizationModule
- Les "security attributes"

Exemples de travaux pratiques (à titre indicatif)

- *Créer un outil d'authentification avec HTTP basic*
- *Proposer des mesures de sécurisation*
- *Implémenter certaines des mesures proposées*

Jour 2 – Après-midi

La sécurité applicative

- Anatomie d'une faille applicative
- Principales vulnérabilités de sécurité courantes dans les applications .NET et C#
- Présentation de l'OWASP
- Les Security Cheat Sheets
- Les guides de l'OWASP (Test Guide, Dev Guide...)
- L'ASVS (Application Security Verification Standard)
- Les grandes familles de vulnérabilités
 - Les CVE (Common Vulnerabilities and Exposures)
 - Les CWE (Common Weakness Enumerations)
 - Le scoring CVSS (Common Vulnerability Scoring System)

Exemples de travaux pratiques (à titre indicatif)

- *Estimation de la vulnérabilité d'un produit*
- *Exploitation :*
 - *D'une injection d'entête HTTP*
 - *D'une injection SQL*
 - *D'une Cross-Site Scripting*
 - *D'une Cross-Site Request Forgery*

- *D'une Server-Side Request Forgery*

Jour 3 – Matin

Exemples de travaux pratiques (à titre indicatif) - Suite

- *Exploitation d'un vol de session*
- *Exploitation d'une désérialisation*
- *Exploitation d'une référence directe à un objet*

La sécurité du code externe

- Le cas des librairies
- Le cas des API

Jour 3 – Après-midi

Mettre en place du Secure Code

- Durcir son application avec l'OWASP ASVS et l'OWASP Dev Guide
- Les bonnes pratiques de sécurisation du code
- Validation et filtrage des entrées utilisateur
- Se protéger de la décompilation
- L'obfuscation du code
- Faire des tests et des validations
 - La capture via proxy
 - La capture via tcpdump ou Wireshark
 - Les tests avec Postman
 - Les vulnerability scanners
- Le DAST (Dynamic Application Security Testing)
- Le SAST (Static Application Security Testing)
- Filtrer les échanges
 - Les WAF (Web Application Firewalls)
 - Les IPS et les IDS
- Limiter l'exposition
 - Rôle des firewalls, proxies et DMZ
- Outils et technologies de sécurité (Firewall, IPS, IDS...)

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](#)

Détails de la session

Du 5 janvier 2027 au 7 janvier 2027 (3 jours / 21 heures)

À distance

Du 5 janvier 2027 au 7 janvier 2027

À distance

- 5 janvier 2027 9h00 – 16h00
- 6 janvier 2027 9h00 – 16h00
- 7 janvier 2027 9h00 – 16h00