

Sécurisez vos applications .net

Dans cette formation, vous apprendrez à sécuriser vos applications .NET et les ressources associées (IIS, SQL Server).

OBJECTIFS

- Comprendre l'importance de la sécurité ;
- Présenter et expliquer les failles de sécurité ;
- Concevoir et développer des applications .NET sécurisées ;
- Déceler les principales failles de sécurités dans les applications .NET, et apporter des solutions appropriées.

PROGRAMME

Présentation de la sécurité dans les applications .NET

- L'importance de la sécurité
- Contre qui et quoi se défendre ?
- Les failles de sécurité classiques
- Comment une attaque survient ?
- Les challenges de la sécurité

Conseils pour la création d'applications .NET sécurisées

- Se protéger contre les attaques courantes
- Réduire la surface d'attaque
- Se méfier des données des utilisateurs
- Gérer correctement les erreurs
- Tester la sécurité
- Utiliser le Dotfuscator
- Signer les assemblies
- Travaux pratiques :
 - > Décompilation et altération d'une assembly non signée
 - > Mise en œuvre d'un code de piratage d'une application

Modélisation des menaces dans les applications .NET

- Chronologie de développement d'une application sécurisée
- Processus de modélisation des menaces

Validation des données dans les applications Web

- Identifier les sources de données
- Attaques par les cookies, HTTP et JavaScript Injection
- Les contrôles de validation de données
- Gestion des erreurs
- Travaux pratiques :
 - > Attaque par injection de JavaScript
 - > Attaque par soumission de formulaire non sécurisé côté serveur
 - > Attaque d'un site web et provocation d'un déni de service

Authentification Server Web IIS

0 jour

prix par participant

0 €HT

code formation : IN326

option restauration

18 € par jour

LES + TANIT FORMATION

- Remise d'un support de cours et/ou un manuel de référence au format numérique ou papier Mise en pratique au travers d'exercices et de cas concrets réalisés seul ou en groupe
- L'évaluation des acquis se fait tout au long de la formation au travers des différents travaux dirigés réalisés par le stagiaire
- Formateur professionnel de l'informatique et de la pédagogie (compétences techniques et pédagogiques certifiées)
- Formation dans une salle équipée d'une solution de visio-conférence dans le cas des formations suivies "présentiel à distance"
- Le nombre de stagiaires peut varier de 5 à 6 personnes en moyenne, ce qui facilite le suivi permanent et la proximité avec chaque stagiaire.

POUR QUI ?

- Développeurs, analystes programmeurs, chefs de projets.

PRÉ-REQUIS

- Idéalement, avoir suivi les formations " Les fondamentaux du développement .NET avec le langage C# 7 sous Visual Studio 2017 " et " Développer des applications Web ASP.NET Core MVC en C# sous Visual Studio 2017 ", ou posséder les connaissances et compétences équivalentes.

- Importance de la protection des serveurs Web
- Authentification et Autorisations
- Restreindre l'accès aux applications Web
- Permissions sur les applications Web dans IIS
- Les modes d'authentification
- L'authentications OAuth2
- Scénarii d'authentification dans une application
- Intranet/Internet
- Emprunt d'identité et délégation
- Gestion de l'identité de l'utilisateur
- Améliorations de la sécurité dans IIS
- Travaux pratiques :
 - > Sécuriser un site Web.
 - > Configurer correctement IIS pour l'hébergement d'une application Web

Sécuriser une application ASP.NET et ses ressources

- Présentation
- Authentification Windows et personnalisée
- Gestion des autorisations
- L'API de sécurité du Framework .NET
- Traitement des requêtes HTTP
- Créer un handler HTTP personnalisé
- Travaux pratiques :
 - > Sécuriser le fichier web.config et crypter les données sensibles
 - > Mettre en place les directives appropriées de sécurisation applicative
 - > Observation des requêtes GET et POST, mise en place d'un sniffer de trames réseaux

Concepts de sécurité basée sur les rôles

- Présentation
- Identités et entités de sécurité
- Création d'identités et d'entités de sécurité Windows
- Création d'identités et d'entités de sécurité génériques
- Vérification de l'identité et de sécurité

Sécurité d'accès au code

- Présentation
- Sécurité d'accès au code dans une application .NET
- Bases fondamentales de la sécurité d'accès au code
- Vérifications de sécurité
- Travaux pratiques :
 - > Création d'une application et mise en place des politiques de sécurité
 - > Accès aux ressources basées sur les rôles

Sécuriser l'accès aux bases de données SQL Server

- Scénarii d'authentification SQL Server
- Choix d'authentification sous SQL Server
- Les chaînes de connexion et pools de connexions
- Crypter le fichier de configuration
- Les attaques SQL Injection
- Travaux pratiques : Mise en œuvre d'une application se connectant aux données

SESSIONS

et mise en œuvre des conditions d'injection SQL puis correction de la faille de sécurité

Protéger les données, leur transfert et leur l'intégrité

- Introduction à la cryptographie
- Cryptage, hachage et signature
- Cryptage symétrique et asymétrique
- Vérifier l'intégrité des données avec le hachage
- Communication sécurisée avec SSL
- Les API de cryptage et de protection de données
- Cryptographie dans le Framework .NET
- Les limites de la classe String et la classe SecureString
- Travaux pratiques :
 - > Mise en œuvre d'un cryptage Rijndael
 - > Mise en œuvre d'une politique de vérification de l'intégrité des données basées sur la hashage

Les jetons de sécurité

- Jetons : UserName Token, Binary Token
- JWS
- Certificat X.509

Sécurité et développement Web

- Classification des attaques : STRIDE, OWASP
- Les erreurs classiques
- Attaque par injection
- XSS (Injection croisée de code)

Tester la sécurité des applications .NET

- Scénarios de tests
- Créer un plan de test de sécurité
- Trouver les interfaces à tester
- Tester l'authentification, les autorisations
- Tester les pages ASP .NET

STAGE / FORMATION

Intitulé _____
Code _____
Date _____ Lieu _____
Prix HT _____ + TVA (taux en vigueur de 20%) _____ Prix TTC _____
Nombre de repas _____ Prix total des repas _____

BULLETIN D'INSCRIPTION

ENTREPRISE

Raison sociale _____
N° SIRET _____ N° TVA _____ Effectif _____
Adresse _____
Tél. _____ Fax. _____

Responsable Formation

M. Mme
Nom _____ Prénom _____
Fonction _____ Tél.(ld) _____
Email _____

PARTICIPANTS

M. Mme
Nom _____ Prénom _____
Fonction _____ Tél.(ld) _____
Email _____

FACTURATION / FINANCEMENT

Adresse de facturation (indispensable)

Un numéro de bon de commande interne à votre entreprise doit-il
apparaître sur votre facture ?

Oui Non

Si oui, numéro _____

Le financement de votre formation passera-t-il par un OPCA ?

Oui Non

Numéro de prise en Charge _____

Adresse de votre OPCA _____

RÈGLEMENT

Ci-joint un chèque de _____ € TTC
(à l'ordre de Tanit Formation)

Par virement à notre banque :

CIC PARIS MOGADOR

FR76 3006 6107 4100 0200 8570 337

BIC : CMCIFRPP

Nom _____

Prénom _____

Date _____

Signature et cachet de l'entreprise (obligatoire)

Si l'accord de prise en charge de l'OPCA ne parvient pas à Tanit Formation au premier jour de la formation, Tanit Formation se réserve le droit de facturer la totalité des frais de formation au client.