Ambient IT
128 Boulevard Macdonald
75019 Paris

Mail : formation@ambient-it.net
Tél : +33 (0)1 40 34 11 53

AMBIENT-IT

Formation Sécurité OWASP

Durée 2 jours (14 heures)

Présentation

Formation avancée sur la sécurité applicative Web .NET / ASP.NET 4.8 MVC / Core 3.1. Cette formation vous présentera les bonnes pratiques à adopter afin d'éviter la plupart des failles de sécurités récentes (TOP 10 OWASP 2017).

Formez-vos aux bonnes pratiques concernant la sécurité et les failles software. Sécurisez votre solution SaaS et vos applicatifs Web ASP.NET. Évitez les failles potentielles et les alertes d'audits.Instaurer une culture et une sensibilisation à la sécurité dans vos équipes d'ingénierie, afin de les rendre autonomes sur les bons réflexes et les best practices à mettre en place.

Notamment en priorité sur les principes d'OWASP (TOP 10 des failles de sécu), de type : Cross-site Scripting (XSS), Injection flaws, Broken Auth&Acess, CSRF, API provider, Data Encodage, Signature & Chiffrement...

L'objectif est de pouvoir prévenir les vulnérabilités potentielles et de les corriger en utilisant une bonne méthodologie. N'attendez pas qu'il ne soit trop tard pour sensibiliser votre équipe aux meilleurs techniques de prévention !

Dans cette formation sur l'état de l'art en matière de sécurité applicative, vous utiliserez évidement les dernières technologies : C# 9, Visual Studio 2019, Core 3.1.

Objectifs

- Connaître et comprendre les failles les plus courantes sur le Web
- Connaître les mécanismes de sécurité de .NET
- Acquérir les réflexes pour développer des applications sécurisées
- Authentifier et autoriser l'accès aux applications ASP .NET
- Chiffrer des données avec le framework .NET

Public visé

- Développeurs
- Architectes
- Auditeurs en sécurité

Pré-requis

Avoir des connaissances en programmation C#, .NET.

Pour aller plus loin

- Nous proposons également une formation sur la nouvelle version Core de .Net sur ASP

Programme de notre formation Sécurité OWASP .NET

Les principales failles de sécurité

- Présentation des plus grosses failles 2018 & 2019 et leurs coûts respectifs (Aadhar, Cambridge Analytica, Exactis, Marriott Starwood...)
- OWASP Top 10 des failles de sécurité en 2017
- Exploitation des failles
- Notion et calcul du Risk Factor
- Visualisation de l'impact utilisateur
- Mise en œuvre des mécanismes de sécurité

Cas pratiques

- Injection SQL
- Broken Authentification
- Hashing & Salting
- Sensitive data exposure
- Security Misconfiguration
- Xml External Entities (XXE)
- Broken Access Control
- Cross Site Scripting (XSS)
- Insecure deserialization
- Insufficient Logging & Monitoring
- Using Components with Known Vulnerabilities
- CORS (Cross-origin resource sharing)
- CSRF (Cross Site Request Forgery)
    - SameSite Cookie
    - Unvalidated redirect

La sécurité au quotidien

- Présentation d'outils d'analyse

- Créer son propre analyser Roslyn
  - Linq : requêter sur l'arbre syntaxique
  - Code Analyzer 101
  - Diagnostic Analyzer Class
  - Analysis Context Event
- Puma
- Culture de la sécurité

Les certificats

- Intérêt et fonctionnement des certificats serveurs
- Intérêt, fonctionnement et mise en œuvre des certificats clients
- Intérêt, fonctionnement et mise en œuvre du pinning de certificat

Le chiffrement

- Présentation des différents types et algorithmes de chiffrement
  - Symétrique
  - Asymétrique : HMAC, JWT, AES, PBKDF2, BASE64
  - Signature numérique
  - TLS, SSL
  - Pinning
- Mise en œuvre en .NET

Sociétés concernées

Cette formation s'adresse aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée.

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 multiple permet de vérifier l'acquisition correcte des compétences.

Sanction

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