ENI Service

référence
TACNUM1-1D

21h

Sécurité des applications

Mise à jour
17 juillet 2023

2100 € HT

(Télé-)présentiel

TOP FORMATION

Sécurité des applications

Objectifs

- Appréhender l'importance de la sécurité
- Présenter et expliquer les failles de sécurité, les différents types d'attaques et vulnérabilités des applications
- Concevoir et développer des applications sécurisées
- Appréhender les différents principes relatifs à la sécurité dans les plateformes de développement logiciel et les mettre en oeuvre
- Déceler les principales failles de sécurités dans les applications et apporter des solutions appropriées
- Appréhender et mettre en oeuvre les bonnes pratiques de codage permettant d'éviter les failles de sécurité dans une application Web
- Mettre en place une stratégie de veille technologique pour anticiper les potentielles problématiques de sécurité sur les applications existantes

Pré-requis

Posséder une expérience pratique du développement d'applications Web quel que soit le langage de programmation

Public

Développeurs, analystes programmeurs, chefs de projets techniques, architectes

Programme de la formation

Principes de base de la sécurité des applications (1,75 heure)

- L'importance de la sécurité
- Contre qui et quoi se défendre ?
- Les failles de sécurité classiques
- Comment une attaque survient ?
- Les défis de la sécurité
  - Identification : les différentes méthodes
  - Autorisation et permissions d'accès
  - Confidentialité : les mécanismes de cryptage

Les bonnes pratiques (1,75 heure)

- Les patterns de programmation
- La gestion des mots de passe
  - Fonctionnalités de cryptage disponibles dans les plateformes de développement
- Les frameworks
  - La prise en charge des contre-mesures dans les librairies et frameworks applicatifs
- Travaux pratiques :
  - Présentation de librairies et frameworks et de leurs fonctionnalités natives pour la sécurisation des applications dans les différentes plateformes de développement

Sécuriser l'accès aux bases de données (3,5 heures)

- Scénarii d'authentification vers une base de données
- Les chaînes de connexion et pools de connexions
- Crypter les fichiers de configuration
- Les attaques par injection SQL
  - Différentes techniques pour s'en prémunir
- Travaux pratiques :
  - Mise en oeuvre d'une application se connectant aux données et mise en oeuvre des conditions d'injection SQL, puis correction de la faille de sécurité

La sécurité informatique dans un contexte Web (7 heures)

- Le projet OWASP (Open Web Application Security Project)
  - Présentation du projet
  - Analyse des préconisations et bonnes pratiques du référentiel OWASP
- Les différentes attaques et vulnérabilités des applications et sites Web
  - CSRF, XSS, SQL Injection, Remote Code Injection
- 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
- Présentation des attaques et des contre-mesures associées
  - La théorie des techniques de contre-mesure
  - L'apport des frameworks de développement Web pour la sécurité
- Travaux pratiques :
  - Importation d'un projet d'application Web
  - Identification des failles dans l'application
  - Définition de la stratégie de sécurisation
  - Attaque par injection de JavaScript
  - Attaque par soumission de formulaire non sécurisé côté serveur
  - Observation des requêtes GET et POST, mise en place d'un sniffer de trames réseaux

Authentification et autorisations dans les applications Web (3,5 heures)

- Les différents modes d'authentification
  - Basic, Digest, Client-Cert, ...
- Scénarii d'authentification dans une application Intranet/Internet
- Authentification des applications clientes JavaScript
  - Principes et contraintes pour les applications distantes
  - Les mécanismes d'authentification : OAuth2, JSON Web Token, ...
- Autorisations : les rôles de sécurité
  - Définition et déclaration
  - Principes de mappage avec l'existant
- Stratégie de sécurité des différents types d'applications
- Paramétrage d'un conteneur Web/d'applications pour la sécurité
- Paramétrage d'un référentiel d'authentification
- Travaux pratiques :
  - Sécuriser un site Web
  - Déclaration d'une stratégie de restriction d'accès aux URLs dans une application Web
  - Configuration d'un serveur pour l'authentification

Protéger les données, leur transfert et leur intégrité (1,75 heures)

- Introduction à la cryptographie et au chiffrement
- Cryptage, hachage et signature
- Chiffrement symétrique et asymétrique
- Vérifier l'intégrité des données avec le hachage
- Communication sécurisée avec SSL
- Les API de cryptage, de chiffrement et de protection de données
- Travaux pratiques :
  - Mise en oeuvre d'un cryptage de données sensibles (mot de passe, ...)
  - Mise en oeuvre d'une politique de vérification de l'intégrité des données basées sur le hachage
  - Chiffrement de données échangées sur le réseau : HTTPS
  - Configurer l'accès HTTPS d'un serveur

Sécurité d'accès au code (1 heure)

- Présentation
- Sécurité d'accès au code dans une application
- Bases fondamentales de la sécurité d'accès au code
- Vérifications de sécurité
- Décompilation, protection et obfuscation de code

- Travaux pratiques :
  - Création d'une application et mise en place des politiques de sécurité
  - Présentation de la décompilation de byte-code
  - Présentation d'une solution de brouillage de code

Sécurité applicative et veille technologique (1 heure)

- La nécessité d'une surveillance permanente
  - Les bases de connaissances en sécurité applicative
  - Mise en place d'un référentiel de sécurité pour la veille
- Créer un plan de test de sécurité
  - Stratégie, implémentation et fréquence d'usage
- Intégrer les correctifs de sécurité dans les opérations de maintenances applicatives
- Travaux pratiques :
  - Création d'un plan de test de sécurité sur une application sécurisée

Délais d'accès à la formation

Les inscriptions sont possibles jusqu'à 48 heures avant le début de la formation.
Dans le cas d'une formation financée par le CPF, ENI Service est tenu de respecter un délai minimum obligatoire de 11 jours ouvrés entre la date d'envoi de sa proposition et la date de début de la formation.

Modalités et moyens pédagogiques, techniques et d'encadrement

Formation avec un formateur, qui peut être suivie selon l'une des 3 modalités ci-dessous :
1 Dans la salle de cours en présence du formateur.
2 Dans l'une de nos salles de cours immersives, avec le formateur présent physiquement à distance. Les salles immersives sont équipées d'un système de visio-conférence HD et complétées par des outils pédagogiques qui garantissent le même niveau de qualité.
3 Depuis votre domicile ou votre entreprise. Vous rejoignez un environnement de formation en ligne, à l'aide de votre ordinateur, tout en étant éloigné physiquement du formateur et des autres participants. Vous êtes en totale immersion avec le groupe et participez à la formation dans les mêmes conditions que le présentiel. Pour plus d'informations : Le téléprésentiel notre solution de formation à distance.

Le nombre de stagiaires peut varier de 1 à 12 personnes (5 à 6 personnes en moyenne), ce qui facilite le suivi permanent et la proximité avec chaque stagiaire.
Chaque stagiaire dispose d'un poste de travail adapté aux besoins de la formation, d'un support de cours et/ou un manuel de référence au format numérique ou papier.
Pour une meilleure assimilation, le formateur alterne tout au long de la journée les exposés théoriques, les démonstrations et la mise en pratique au travers d'exercices et de cas concrets réalisés seul ou en groupe.

Modalités d'évaluation des acquis

En début et en fin de formation, les stagiaires réalisent une auto-évaluation de leurs connaissances et compétences en lien avec les objectifs de la formation. L'écart entre les deux évaluations permet ainsi de mesurer leurs acquis.
En complément, pour les stagiaires qui le souhaitent, certaines formations peuvent être validées officiellement par un examen de certification.
Les candidats à la certification doivent produire un travail personnel important en vue de se présenter au passage de l'examen, le seul suivi de la formation ne constitue pas un élément suffisant pour garantir un bon résultat et/ou l'obtention de la certification.
Pour certaines formations certifiantes (ex : ITIL, DPO, ...), le passage de l'examen de certification est inclus et réalisé en fin de formation. Les candidats sont alors préparés par le formateur au passage de l'examen tout au long de la formation.

Moyens de suivi d'exécution et appréciation des résultats

Feuille de présence, émargée par demi-journée par chaque stagiaire et le formateur.
Evaluation qualitative de fin de formation, qui est ensuite analysée par l'équipe pédagogique ENI.
Attestation de fin de formation, remise au stagiaire en main propre ou par courrier électronique.

Qualification du formateur

La formation est animée par un professionnel de l'informatique et de la pédagogie, dont les compétences techniques, professionnelles et pédagogiques ont été validées par des certifications et/ou testées et approuvées par les éditeurs et/ou notre équipe pédagogique.
Il est en veille technologique permanente et possède plusieurs années d'expérience sur les produits, technologies et méthodes enseignés.
Il est présent auprès des stagiaires pendant toute la durée de la formation.