Sécurité applicative Java

Présentation

Cette formation vous enseignera les vulnérabilités de sécurité les plus courantes dans les applications Java et comment écrire un code plus robuste et plus sûr. Vous apprendrez le top 10 de l'OWASP et les vulnérabilités typiques du Web en vous concentrant sur la façon dont ces problèmes affectent les applications Web Java dans toute la stack.

Durée : 21,00 heures (3 jours)
Tarif INTRA : Nous contacter

Objectifs de la formation

- Comprendre les problèmes de sécurité des applications web
- Apprendre les exigences PCI-DSS et le développement sécurisé
- Analyser les dix éléments principaux de l'OWASP
- Replacer la sécurité des applications Web dans le contexte de Java
- Comprendre l'importance de la veille technologique et la proactivité dans la démarche de sécurisation
- Gérer les problèmes de sécurité dans votre code Java
- Identifier les vulnérabilités et leurs conséquences
- Apprenez les meilleures pratiques de sécurité en Java

Prérequis

- Expérience du développement Java.

Public

- Développeurs
- Pentesters

Programme de la formation

Introduction

Les bases de la cybersécurité

Docaposte Institute
45-47 Boulevard Paul Vaillant Couturier, 94200 Ivry-sur-Seine
Tél : 01 56 29 70 01 - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de Région Île-de-France

- Qu'est-ce que la sécurité ?
- Menaces et risques
- Types de menaces de cybersécurité
- Conséquences des logiciels non sécurisés
  - Les contraintes et le marché
  - Le côté obscur
- La cybersécurité dans le secteur financier
  - La sécurité des logiciels dans le monde de la finance
  - Menaces et tendances dans le domaine des technologies de pointe

Norme PCI-DSS

- Un aperçu de la norme PCI-DSS
- Les ressources de la norme PCI-DSS
- Exigences PCI-DSS et développement sécurisé
- Développer et maintenir des systèmes et des applications sécurisées
- S'attaquer aux vulnérabilités communes du développement

Le Top 10 de l'OWASP (Partie I)

- Top 10 de l'OWASP - 2017
- Authentification frauduleuse
  - Les bases de l'authentification
  - Faiblesses d'authentification
  - Étude de cas - Equifax Argentine
  - L'usurpation d'identité sur le Web
  - Étude de cas - Contournement de la double authentification de PayPal
  - Les bonnes pratiques en matière d'interface utilisateur
  - Étude de cas - Divulgation d'informations dans Simple Banking pour Android
  - Gestion des mots de passe
- Exposition aux données sensibles
  - Exposition des informations
  - Exposition par extraction de données et agrégation
  - Étude de cas - Exposition des données de l'application Strava fitness
  - Fuite d'informations sur le système
  - Bonnes pratiques en matière d'exposition à l'information
- Utilisation de composants présentant des vulnérabilités connues
  - Utilisation de composants vulnérables

Docaposte Institute
45-47 Boulevard Paul Vaillant Couturier, 94200 Ivry-sur-Seine
Tél : 01 56 29 70 01 - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de Région Île-de-France

- Évaluer l'environnement
- Durcissement
- Importation de fonctionnalités non fiables
- Importation de JavaScript
- Étude de cas - La brèche des données de British Airways
- Étude de cas - La brèche des données d'Equifax
- Gestion de la vulnérabilité

Le Top 10 de l'OWASP (Partie II)

- Injection
  - Principes d'injection
  - Attaques par injection
  - Injection SQL
  - Bonnes pratiques en matière d'injection SQL
  - Injection de code
  - Bonnes pratiques d'injection de commande OS
  - Utilisation de Runtime.exec()
  - Utilisation de ProcessBuilder
  - Étude de cas - Shellshock
  - Étude de cas - Injection de modèle dans Shopify menant à un RCE
  - Les meilleures pratiques en matière d'injection
- Authentification défaillante
  - Gestion des sessions
  - Les bonnes pratiques CSRF
- Entités externes XML (XXE)
  - La définition de type de documents (DTD) et les entités
  - Expansion des entités
  - Attaque d'une entité externe (XXE)
- Scripting intersites (XSS)
  - Les bases des scripts intersites
  - Types de scripts intersites
  - Étude de cas - XSS dans les comptes Fortnite
  - Bonnes pratiques en matière de protection XSS

La sécurité des applications web au-delà du top 10

Docaposte Institute
45-47 Boulevard Paul Vaillant Couturier, 94200 Ivry-sur-Seine
Tél : 01 56 29 70 01 - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de Région Île-de-France

- Sécurité côté client
- Le Tabnabbing
- Le Frame sandboxing

Faiblesses habituelles de sécurité des logiciels

- Validation des entrées
  - Principes de validation des entrées
- Problèmes de traitement des nombres entiers
  - Représentation des entiers signés
  - Visualisation des nombres entiers
  - Overflow des nombres entiers
  - Confusion nombres signés / non signés en Java
  - Troncature des nombres entiers
- Bonnes pratiques
- Autres problèmes numériques
  - Division par zéro
  - Travailler avec des nombres à virgule flottante
- Réflexions dangereuses
  - Réflexions sans validation
- Code natif dangereux
  - Dépendance au code natif
  - Bonnes pratiques pour le traitement du code natif

Caractéristiques de sécurité

- Sécurité de la plate-forme Java
  - Le langage de programmation Java et l'environnement d'exécution
  - Sûreté et sécurité du typage
  - Caractéristiques de sécurité du JRE
  - Le ClassLoader et le BytecodeVerifier
  - Contrôle d'accès au niveau de l'application en Java
  - Contrôle d'accès basé sur les rôles
  - Protéger le code et les applications Java
- Qualité du code
  - Constructeurs et destructeurs
  - Cycles d'initialisation des classes
  - Labo - Cycles d'initialisation

Docaposte Institute
45-47 Boulevard Paul Vaillant Couturier, 94200 Ivry-sur-Seine
Tél : 01 56 29 70 01 - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de Région Île-de-France

- Ressource non diffusée
- La méthode finalize() - les bonnes pratiques
- Les pièges de la programmation orientée objet

- Sérialisation
  - Sérialisation des données sensibles
  - Les bonnes pratiques en matière de sérialisation
  - Désérialiser les flux non fiables
  - Désérialiser les meilleures pratiques
  - Utilisation de ReadObject
  - Objets scellés
  - Regarder vers l'avenir : la désérialisation
  - Programmation axée sur la propriété (POP)

Conclusion

- Des principes de développement sûr
  - Les principes d'une programmation robuste par Matt Bishop
  - Les principes de conception sécurisée de Saltzer et Schröder

Et maintenant ?

- Autres sources et lectures
- Ressources Java

Organisation

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes.

Moyens pédagogiques et techniques

- Apports didactiques pour apporter des connaissances communes.

Docaposte Institute
45-47 Boulevard Paul Vaillant Couturier, 94200 Ivry-sur-Seine
Tél : 01 56 29 70 01 - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de Région Île-de-France

- Mises en situation de réflexion sur le thème du stage et des cas concrets.
- Méthodologie d'apprentissage attractive, interactive et participative.
- Equilibre théorie / pratique : 60 % / 40 %.
- Supports de cours fournis au format papier et/ou numérique.
- Ressources documentaires en ligne et références mises à disposition par le formateur.
- Pour les formations en présentiel dans les locaux de Softeam, les stagiaires sont accueillis dans une salle de cours équipée d'un réseau Wi-Fi, d'un tableau blanc ou paperboard. Un carnet de notes est offert. Un ordinateur avec les logiciels appropriés est mis à disposition (le cas échéant).

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation :

- Recueil des besoins : permet de récolter des informations sur le stagiaire (profil, formation, attentes particulières, ...).
- Auto-positionnement des stagiaires afin de mesurer le niveau de départ.

Tout au long de la formation :

- Évaluation continue des acquis via des questions orales, exercices / projet fil rouge, des QCM, des cas pratiques et mises en situation.

A la fin de la formation :

- Auto-positionnement des stagiaires afin de mesurer l'acquisition des compétences.
- Evaluation du formateur des compétences acquises par les stagiaires.
- Questionnaire de satisfaction à chaud : permet de connaître le ressenti des stagiaires à l'issue de la formation.
- Questionnaire de satisfaction à froid : permet d'évaluer les apports réels de la formation et leurs mises en application au quotidien.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.

Docaposte Institute
45-47 Boulevard Paul Vaillant Couturier, 94200 Ivry-sur-Seine
Tél : 01 56 29 70 01 - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de Région Île-de-France