Formation

DevSec – Top10 OWASP

Durée : 1 jour – 7h

Face aux cyberattaques, l'objectif de la formation DevSec – Top10 OWASP est de fournir aux participants les compétences nécessaires pour concevoir, développer et déployer des applications web résilientes, en intégrant les meilleures pratiques de cybersécurité de l'OWASP.

Celle-ci place l'apprenant dans la peau d'un hacker pour mieux percevoir les conséquences d'une attaque cyber et acquérir les bons réflexes pour s'en protéger.

Une formation pratique sur notre plateforme de simulation *CyberRange* qui alterne théorie et plus de 15 travaux pratiques d'attaques réelles.

Public visé : Développeurs, architectes et experts techniques

Prérequis : Connaissance sur la conception application web (JAVA, JS, .NET, …)

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation, le stagiaire est en capacité de :

- Concevoir et développer des applications robustes en intégrant des mesures de sécurité avancées
- Apprendre les bonnes pratiques de sécurisation dès la phase de développement
- Identifier et corriger les vulnérabilités dans le code et dans les configurations applicatives
- Mettre en œuvre les bonnes pratiques pour garantir l'intégrité et la confidentialité des données sensibles
- Suivre les normes et les réglementations de sécurité informatique et de protection des données
- Mettre en œuvre la supervision et la gestion des incidents pour réagir efficacement aux cyberattaques

PROGRAMME

1. Contrôler les accès (A01 – Broken Access Control)

- Appréhender et exploiter des vulnérabilités sur un manque de contrôle d'accès
- Contourner les contrôles d'accès en modifiant l'URL ou en utilisant un outil d'attaque modifiant les requêtes API
- Manipuler des métadonnées, rejouer ou la falsifier un JSON Web Token (JWT), de cookies ou de champs cachés, afin d'élever les privilèges ou abuser de l'invalidation JWT.
- Mise en place de contre-mesures

Travaux pratiques :

Approche offensive : Exploiter les failles de type IDOR et liées au JWT

Approche défensive : Mettre en place les contre-mesures

Suite =>

Informations pratiques

Durée : 1 jour – 7h

Ressources
Supports de cours
70% d'exercices pratiques

Tarifs 2026
En inter : 990€ HT/stagiaire
En intra : contactez-nous pour un devis

Modalités
Sur inscription
Contact et information par mail
Session de 8 stagiaires minimum

Lieu
Sur site Client, LUPISE
ou distanciel

Accessibilité aux personnes en situation de handicap
Contactez-nous pour étudier la faisabilité de votre demande.

Taux de satisfaction

★ ★ ★ ★ ★

Compétences des formateurs
Nos formateurs sont des spécialistes certifiés de la cybersécurité avec une expérience terrain dans la sécurité des systèmes d'information. Ils ont été validés par notre équipe pédagogique sur le plan des connaissances métiers et sur celui de la pédagogie, et sont évalués régulièrement. Une veille permanente ainsi qu'une pratique régulière dans leur domaine garantit leur niveau d'expertise.

Modalités d'évaluation des stagiaires
Les objectifs sont régulièrement évalués tout au long de la formation moyen de quizz, de mises en situation et de travaux pratiques et formalisés sous forme de grille d'évaluation des compétences en fin de module par le formateur
Le participant complète un test de positionnement en amont et en aval de la formation pour valider les compétences acquises.

Moyens techniques et pédagogiques
Aides audiovisuelles, environnement de formation en ligne, support de cours et exercices, études de cas ou présentation de cas réels, sessions de questions-réponses.

contact@lupise.fr

2. Durcir les moyens cryptographiques (A02 – Cryptographic Failure)

- Gérer des secrets et des certificats
- Rechercher des données en clair et protocoles non sécurisés
- Identifier l'absence de directives/en-têtes de sécurité
- Mise en place de contre-mesures

Travaux pratiques :

Approche offensive : Identifier et Exploiter les failles liées à du chiffrement mal configuré

Approche défensive : Mettre en place les contre-mesures

3. Protéger son application contre les injections (A03/A10 – Injection)

- Les types d'injection à impact serveur : SQL, XXE, RCE, SSRF
- Les types d'injection à impact client : XSS
- Mise en place de contre-mesures

Travaux pratiques :

Approche offensive : Identifier et Exploiter la SQLi, XSS, SSRF, RCE, XXE

Approche défensive : Mettre en place les contre-mesures

4. Renforcer les configurations de sécurité (A05 – Security Misconfiguration)

- Identifier les mauvaises pratiques de configurations de sécurité
- Gérer les services (composants, ports, applications, …)
- Paramétrer la sécurité dans les serveurs d'application et frameworks
- Identifier l'absence de directives/en-têtes de sécurité
- Mise en place de contre-mesures

Travaux pratiques :

Approche offensive : Identifier et exploiter des problématiques de configurations

Approche défensive : Identifier des problématiques de configuration avec un scanner de vulnérabilités

5. Identifier les composants avec vulnérabilités connues (A06 – Vulnerable and Outdated Components)

- Identifier les outils d'analyse de composants
- Identifier des composants sécurisés
- Mise en place de contre-mesures

Travaux pratiques :

Approche offensive : Identifier et exploiter une CVE

Approche défensive : Identifier des problématiques de configuration avec un scanner de vulnérabilités

6. Renforcer la gestion de l'authentification et mécanismes de session (07 – Identification & Authentication Failures)

- Maîtriser les techniques d'attaques automatisées et bruteforcing
- Identifier des composants sécurisés
- Identifier la présence d'identifiants dans les URL
- Gérer les sessions et vol de session
- Mise en place de contre-mesures

Travaux pratiques :

Approche offensive : Bruteforcer un login ; usurper une session

Approche défensive : Mettre en place les contre-mesures

7. Renforcer les systèmes de contrôle et de journalisation (A09 – Security Logging & Monitoring Failures)

- Détecter, alerter et répondre aux incidents
- Mise en place de contre-mesures

Travaux pratiques :

Approche défensive : Gérer une crise cyber

Approche défensive : Investiguer sur une attaque cyber

8. Protéger son application contre la désérialisation non sécurisée

- Injecter des données non fiables
- Accéder à des ressources sensibles et les compromettre
- Mise en place de contre-mesures

Travaux pratiques :

Approche offensive : Identifier et exploiter une vulnérabilité de désérialisation

Approche défensive : Mettre en place les contre-mesures

9. Implémenter l'automatisation de la sécurité - DevSecOps

- Réaliser une approche « Secure by design » et la sécurité en continue
- Disposer d'outils et tester la sécurité
- Intégrer les personnes, les processus, la technologie et la gouvernance.

Informations complémentaires

- **Matériel nécessaire**

Les stagiaires devront être munis d'un PC pendant la formation.

- **Evaluation et validation de la formation**

À la fin de chaque formation, les participants complètent un questionnaire d'évaluation qui est analysé par nos équipes pédagogiques.
Une feuille d'émargement par demi-journée de présence est signée par le stagiaire. A l'issue de la formation, un certificat de réalisation de formation est remis au stagiaire si celui-ci a bien assisté à la totalité de la session.

contact@lupise.fr