Formation « Sécurité des serveurs et des applications Web »

Réf : SECUDEVWEB

L'infrastructure Web expose directement votre société aux menaces externe. Renforcez vos défenses en sécurisant efficacement tous les vecteurs exploités par les attaquants !

Objectifs

- **Éduquer vos équipes de développement aux risques et aux enjeux de la sécurité applicative en mettant en application l'ensemble des points clés du standard OWASP**
- **Être en mesure d'augmenter rapidement la qualité et la sécurité de leurs développements de façon pertinente et efficace.**

Durée & horaires

- **5 jours soit 35 heures**
- **Horaires : 9h30 à 12h et de 13h30 à 17h30/18h00.**

Nombre de participant

- **Minimum 8 participants – Maximum 24 participants**

Public visé

- **Personnes ayant un profil technique souhaitant acquérir les connaissances suffisantes pour sécuriser leurs développements Web :**
  - **DevSecOps**
  - **Programmeurs,**
  - **Développeurs**
  - **Architectes**
  - **Chefs de projet**
  - **Consultants cybersécurité**

Pré-requis

- **Expérience en programmation, idéalement en développement Web**
- **Connaissance de base en cybersécurité, par exemple suivi de la formation SECUCYBER est un plus**

Méthode pédagogique

- **Cours magistral illustré par des exercices guidés pas à pas en présentiel et accessible en distanciel via ZOOM (webcam obligatoire)**
- **Résolution de challenges de sécurité réaliste de type Capture The Flag (CTF)**

Supports

- **Support de cours au format papier en français en mode présentiel, au format numérique (après signature d'un engagement de non divulgation) en mode distanciel**
- **Ordinateur portable mis à disposition du stagiaire**
- **Cahier d'exercices et corrections des exercices**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**
- **Evaluation de pré-formation envoyée avant le début de la formation**

- **Evaluation de mi-formation effectuée en session par le formateur au moyen de QCM et de travaux pratiques**
- **Examen final à la fin de la formation (cf certification)**
  Ces évaluations ont pour but de valider les compétences acquises.

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUWEB par HS2.**

Programme

Introduction aux risques et aux enjeux de la sécurité applicative
- Les motivations des attaquants
- Notions d'analyse de risque
- Les grands principes récurrents de la sécurité

Rappels sur les technologies web
- Encodages (URL, HTML, Base64)
- HTTP / HTTPS
- Introduction à un proxy Web pour intercepter, analyser et modifier les échanges HTTP(S)

La sécurité côté client
- Same Origin Policy
- Communication "cross-domain"
- Injection XSS
- Les entêtes de sécurité

Notions de cryptographie
- Rappels sur les primitives de base (chiffrement, hash)
- Cryptographie symétrique, asymétrique et hybride
- Echange de clé
- HSM, carte à puce et TPM
- PKI et certificats
- Réflexion sur la cryptographie post-quantique

Les processus d'authentification et d'autorisation
- Les méthodes d'authentification http
- Authentification forte/double facteur
- Centralisation des méthodes d'authentification/d'autorisation
  - SAML, OpenID, OAuth 2
- Les attaques sur l'authentification
- Durcissement des méthodes d'authentification

La gestion des sessions
- Les jetons de session
- Les cookies
- Forge de requêtes inter-sites (CSRF)
- Fixation de session
- Forge de jetons de session
- Cloisonnement des droits horizontaux et verticaux

Défense de l'application côté serveur
- Principes de base sur les injections
- Injections de commande et de code
- Injection sur les bases de données (SQL, HQL, NoSQL…)
- Utilisation du XML : Injection et XXE

- SSRF
- Désérialisation
- Inclusion de fichiers et injection de templates
- Téléversement (upload) et Path traversal

Gestion des secrets et des données sensibles

- Stockage et politiques de mots de passes
- Secrets dans l'environnement de développement/production
- Auditer la sécurité des mots de passes
- Chiffrement et base de données
- Conformité aux référentiels (données de santé, PCI-DSS, RGPD…)

La sécurité des communications

- HTTPS, SSL, TLS
- Dissection d'une suite cryptographique
- Recommandations
- Audits et contrôles

Webservices et clients lourds

- SOAP, REST : leur fonctionnement et leur sécurité
- Les clients lourds et leur sécurité
    - Angular,, React, Vue…
    - Gestion des permissions et des secrets côté client ?

Sécurité et processus de développement

- Secure SDLC
- Développement sécurisé
- Les tests des fonctions de sécurité
- La sécurité du produit en production
- La gestion des vulnérabilités
- La gestion des patchs
- La gestion des dépendances et des vulnérabilités transitives

Durcissement des services

- Gestion des logs et des erreurs
- Réduction de la surface d'attaque
- Durcissement du socle
- Durcissement du service web