FORMATION EN SÉCURITÉ DES APPLICATIONS ET DES DÉVELOPPEMENTS

Cette formation en sécurité applicative **vous sensibilisera aux risques et aux enjeux de la sécurité applicative** en illustrant l'ensemble des points clés du standard **OWASP** et de son **top 10** des vulnérabilités les plus critiques et répandues sur Internet. Vous serez en mesure d'améliorer et de tester la sécurité de vos applications (et de celles développées par des tiers) de façon pertinente et efficace.

CONTENU DE LA FORMATION

- Introduction aux risques et aux enjeux de la sécurité applicative
- Rappels sur les technologies web
- Introduction aux techniques d'attaque et aux mécanismes de défense
- La phase de reconnaissance utilisée avant d'attaquer une application
- Le mécanisme de gestion de l'authentification (attaque et défense)
- Le mécanisme de gestion de la session (attaque et défense)
- Le mécanisme de gestion des autorisations (attaque et défense)
- La gestion des entrées utilisateurs (injection de code)
- Les attaques ciblant les autres utilisateurs (attaque de type cross-site)
- Sécurité de la journalisation, de la gestion des erreurs et des exceptions
- Sécurité des services web (Frontend JavaScript, API SOAP & REST)
- Introduction à la cryptographie (Chiffrement, Hash, Signature, Certificat, Aléa)

MÉTHODE PÉDAGOGIQUE

- Les parcours de formation sont répétés tous les mois afin de permettre votre inscription à tout moment de l'année.
- Nos sessions de formations sont découpées en bloc de 2 heures et sont dispensées les mardis et jeudis en Téléprésentiel sur 4 semaines.
- Des exercices et travaux pratiques vous permettent de participer activement à la formation. Il s'agit de tester des applications réalistes pour relever des vulnérabilités, en analysant leur code source ou en attaquant directement la version compilée / interprétée. Les laboratoires sont accessibles 24 / 24, 7 jours sur 7.

MODALITÉS DE LA FORMATION

Public visé : Adapté à toutes les parties prenantes avec des compétences techniques liées aux développements d'applications (Chefs de projet / Architectes / Développeurs / Testeurs / etc.)

Formation en télé **présentiel**

Travaux pratiques : **elearning et suivi personnalisé**

Durée de la formation : **16 heures**

Durée des exercices et TP : **jusqu'à 56 heures**

Une attestation **de suivi de la formation nominative est délivrée à chaque stagiaire.**

PROGRAMME DÉTAILLÉ DE LA FORMATION

0. Introduction aux risques et enjeux de la sécurité applicative

Quelques idées reçues
La couche applicative – Une surface d'attaque de choix
Prise en main de la salle de classe virtuelle Prise en main du lab et de la plateforme de challenges de sécurité pour les exercices et les travaux pratiques

1. Rappels sur les technologies Web

Encodages (URL, HTML, Base64)
HTTP / HTTPS
Utilisation d'un proxy Web pour intercepter, analyser et modifier les échanges HTTP(S)

2. Introduction aux techniques d'attaque et aux mécanismes de défense

Présentation de l'OWASP (guides, outils et standard TOP 10 de l'OWASP Web)
Attaques et mécanismes de défense
Utilisation du scanner de vulnérabilité OWASP ZAP

3. Connaissance de l'application

Axes de fuite d'informations techniques
Utilisation d'outils de "Crawling" et d'outils de collecte d'information

4. Authentification

Mécanismes d'authentification les plus rencontrés
Failles / Attaques qui ciblent le mécanisme d'authentification
Moyens de défense permettant de sécuriser le mécanisme d'authentification
"Brute-force" d'un mécanisme d'authentification
Interception de données en transit (Sniffing)

5. Gestion des autorisations

Droits horizontaux et droits verticaux
Failles / Attaques qui ciblent le mécanisme de gestion de la session d'information
Attaques de type Cross-Site Request Forgery (CSRF)
Attaques de type File Inclusion (RFI / LFI) et Path Traversal
Moyens de défense permettant de sécuriser le mécanisme de gestion de la session
Exploitation d'une faille de type Path Traversal

6. Injection de code- Gestion des entrées utilisateurs

Les différents types d'attaques permettant l'injection de code (SQL, HQL, LDAP, commandes, etc.) et le principe général de ce type d'attaque
Moyens de défense permettant de sécuriser vos entrées utilisateurs
Exploitation de failles de type Injection SQL manuellement et de façon automatique (via l'utilisation d'un outil)

7. Attaques ciblant d'autres utilisateurs – Gestion

Attaques de type Cross-Site Scripting (XSS)
Le cas des clients riches JavaScript (Angular, Backbone, Ember, NodeJS, ReactJS, etc.)
Moyens de défense permettant de sécuriser la navigation de vos utilisateurs et de se protéger contre l'injection de code HTML / JavaScript
Mise en œuvre de différents scénarios d'attaques reposant sur l'exploitation d'une faille de type Cross-Site Scripting (modification de l'affichage, vol de session, redirection arbitraire, etc.)

8. Journalisation des évènements de sécurité

Principe et enjeux de la journalisation des évènements de sécurité
Stockage d'informations sensibles dans les journaux et attaques de type injection de « logs »
Axes de prévention et bonnes pratiques dans le domaine

9. Introduction à la cryptographie

Principes de base de la cryptographie (chiffrement symétrique et asymétrique, « Hashage », Signature, certificat)
Bonnes pratiques dans le domaine

10. Gestion des erreurs et des exceptions

Principe et enjeux de la gestion des erreurs et des exceptions
Axes de prévention et bonnes pratiques dans le domaine

11. Sécurité des sites Web

Front-end à base de clients riches JavaScript
Les failles des clients riches JavaScript
Services Web SOAP et REST
Failles des Services Web SOAP et des services REST
Axes de prévention et bonnes pratiques dans le domaine