Formation Sécurité des applications

Mettre en oeuvre les règles et bonnes pratiques liées au développement sécurisé d'applications

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Les applications web sont de plus en plus exposées aux tentatives de piratages. La sécurisation d'une application et des données qu'elle véhicule fait dorénavant partie intégrante de tout nouveau projet de développement. Tous les acteurs IT ont pris conscience de cette nécessité et intègrent dans leurs solutions des éléments et des outils offrant un niveau de sécurisation à la hauteur des enjeux et attentes du marché. Durant cette formation de 3 jours, les participants aborderont dans le détail chaque brique de sécurisation qu'il est possible de considérer et s'approprieront les techniques à employer pour renforcer la sécurité de leurs prochaines applications.

Référence	PRG303
Durée	3 jours (21h)
Tarif	2 190 €HT

Objectifs

| Identifier les problématiques de sécurité des applications
| Identifier les principales menaces et vulnérabilité
| Expliquer les méthodologies / technologies de protection et de contrôle de la sécurité des applications
| Mettre en place une stratégie de veille

Public

| Architectes
| Développeurs
| Analystes
| Chefs de projets...

Prérequis

| Disposer d'une bonne connaissance de la programmation objet et de la programmation d'applications Web

Programme de la formation

Sécurité dans le Framework et du code
| Concepts fondamentaux
| Sécurité d'accès du code et des ressources
| Sécurité basée sur les rôles
| Le principe du W^X
| Services de chiffrement
| Validation et contrôle des entrées / sorties
| Gestion et masquage d'erreurs
| Gestion sécurisée de la mémoire
| Contrôle d'authenticité et d'intégrité d'une application/d'un code
| Offuscation du code
| Reverse engineering sur : bundle C#, application Java, binaire Windows
| Contrôle des droits avant exécution du code
| Sécuriser les données sensibles présentes dans un binaire
| Stack/Buffer/Heap overflow

Les bases de la cryptographie
| Cryptographie - Les définitions
| Types de chiffrement : chiffrement à clés partagées, chiffrement à clé publique

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
du 15 au 17 septembre 2025
du 3 au 5 novembre 2025

PARIS
du 15 au 17 septembre 2025
du 3 au 5 novembre 2025

AIX-EN-PROVENCE
du 3 au 5 novembre 2025

BORDEAUX
du 15 au 17 septembre 2025
du 3 au 5 novembre 2025

GRENOBLE
du 15 au 17 septembre 2025
du 3 au 5 novembre 2025

LILLE
du 15 au 17 septembre 2025

LYON
du 15 au 17 septembre 2025
du 3 au 5 novembre 2025

NANTES
du 15 au 17 septembre 2025

RENNES
du 15 au 17 septembre 2025

VOIR TOUTES LES DATES

| Symétrique vs. asymétrique, combinaisons symétrique / asymétrique
| Fonctions de hachage
| Utilisation des sels
| Signatures numériques, processus de signature, processus de vérification

Chiffrement, hash et signature des données
| Cryptographie Service Providers (CSP)
| System, security, cryptographie
| Choix des algorithmes de chiffrement
| Chiffrement symétrique : algorithme (DES, 3DES, RC2, AES), chiffrement de flux, mode de chiffrement (CBC, ECB, CFB)
| Algorithmes asymétriques
| Algorithme : RSA, DSA, GPG
| Algorithme de hachage : MD5, SHA1 / SHA2 / SH3

Vue d'ensemble d'une infrastructure à clé publique (PKI)
| Certificat numérique : certificat X.509
| PKI - Les définitions
| Les fonctions PKI
| PKI - Les composants
| PKI - Le fonctionnement
| Applications de PKI : SSL, VPN, IPSec
| IPSec et SSL en entreprise
| Smart Cards (cartes intelligentes)
| Autorité de certification

SSL et certificat de serveur
| Certificat de serveur SSL : présentation, autorité de certification d'entreprise, autorité de certification autonome

Utilisation de SSL et des certificats clients
| Certificats clients
| Fonctionnement de SSL : phase I, II, III et IV
| Vérification de la couverture d'utilisation d'un certificat (lors du handshake)
| Vérification des dates d'utilisation d'un certificat

Sécurité des services Web
| Objectifs de la sécurisation des services Web : authentification, autorisation, confidentialité et intégrité
| Limitations liées à SSL
| Sécurité des services Web : WSE 2.0, sécurisation des messages SOAP / REST

Jetons de sécurité
| Jetons de sécurité : User-Name Token, Binary Token, XML Token, JWT (JSON Web Tokens), Session-based Token
| Intégrité d'un jeton (MAC / HMAC)
| Cycle de vie d'un jeton, expiration automatique (ou pas), contexte d'utilisation d'un jeton
| Habilitations suivant le contexte du jeton
| Certificats X.509
| Signature des messages SOAP / REST : création d'un jeton de sécurité, vérification des messages (MAC / HMAC), chiffrement des messages, déchiffrement du message

Sécurité et développement Web
| Classification des attaques : STRIDE, OWASP
| Les erreurs classiques
| Authentification par jeton et gestion des habilitations
| Les handlers et méthodes HTTP
| Séparation des handlers par contexte de sécurité
| Attaque par injection
| Injection HTML
| Injection CSS
| Injection JS
| Injection SQL
| XSS (Injection croisée de code) : XSS réfléchi, XSS stocké
| XSS Cookie Stealer
| CSRF : Cross-Site Request Forgery

Organiser la veille
| Top 10 de l'OWASP
| Le système CVE

HUB Formation - 14 avenue de l'Opéra - 75001 Paris
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.