Cleverinstitut
L'institut de formation continue des professionnels du Web

Formation Sécurité des applications web

Référence formation : SECWEB01
Durée : 2 jours (14 heures)
Prix conseillé : 1 390 € HT (hors promotion ou remise particulière)

Description

La sécurité est la préoccupation et la responsabilité de tous, en particulier sur le web où le nombre et la complexité des menaces ne cessent de croitre.

Cette formation sécurité Web vous apprendra à déceler les points faibles de vos applications web, développer de façon sécurisée et corriger vos vulnérabilités. Vous apprendrez également à superviser l'activité de vos applications web afin de détecter et réagir aux tentatives d'intrusion.

Objectif pédagogique

A l'issue de cette formation, les participants seront en mesure de :

- **Découvrir les menaces Web classiques et modernes.**
- **Savoir repérer vos points faibles.**
- **Savoir corriger vos vulnérabilités et développer de façon sécurisée.**
- **Apprendre à mettre en place et exploiter un système de "monitoring" sécurité afin de détecter et réagir aux tentatives d'intrusion.**

Pré-requis

Connaissances en développement Web : JavaScript / HTTP / HTML / CSS

Public

Chefs de projet Web
Développeurs

Dates des prochaines sessions

Du jeudi 05/04 au vendredi 06/04 2018	Paris	1 390 €
Du jeudi 04/10 au vendredi 05/10 2018	Paris	1 390 €
Du jeudi 06/12 au vendredi 07/12 2018	Paris	1 390 €

Plan de cours

Présentation des menaces, vulnérabilités des applications Web

Présentation des différents efforts de standardisation de la terminologie liée à la sécurité
Typologie des menaces selon le WASC, le top 10 des menaces selon OWASP
Faille applicatives : injection, protection d'URL, faille de référence, stockage non sécurisé
Attaque côté client : Cross Site Scripting (XSS), gestion de session et authentification, attaque CSRF, Phishing…
Faille de configuration : attaques sur les configurations standard
Attaque de type DDOS
Les dangers spécifiques du Web 2.0.

Technologies liées à la sécurité

Firewalls, panorama des outils, techniques de bases réseau
Filtres des requêtes HTTP
Empreinte de message, les algorithmes SHA-x et MD5
Signature numérique, Clé publique/ clé privé, Coffre à clé et coffre de confiance, Autorités de certification
Chiffrement de données, les algorithmes AES et RSA
Protocoles SSL v2/v3 et TLS, PKI, certificats X509,
Techniques d'authentification HTTP, authentification par certificat

Sécuriser les applications Web

Protections basiques : Re-post des données, Time-out et déconnexion, Masquer les URL, Validation des données
Usurpation d'identité : Cookies et certificats numériques, Session ID et jeton de transaction, Détournement
Se protéger des attaques client : XSS ou Cross Site Scripting, Utilisation des références directes, CSRF ou Cross Site Request Forgery, Sécurité d'accès au SGBD, SQL Injection, Utilisation du JavaScript, Échappement des tags HTML
Protections contre les attaques de force brute, Liste de contrôle d'accès

Contrôler la sécurité des applications Web

Test d'intrusion, audit de sécurité, scanners de vulnérabilités
Organiser une veille technologique efficace
Déclaration des incidents de sécurité

Démonstration

Mise en oeuvre d'un serveur Web avec certificat X509 EV : analyse des échanges protocolaires
Exploitation d'une faille de sécurité critique sur le frontal HTTP
Attaque de type HTTPS Stripping

Gestion de la sécurité mobile

Composants d'un système d'exploitation mobile
Risques auxquels sont exposés les appareils mobiles
Les principales menaces pesant sur les appareils mobiles
Étudier les outils de piratage des appareils mobiles
Méthode pour sécuriser les environnements mobiles.

Avant et après la formation

Parce ce que la formation est un moment privilégié de sa carrière professionnelle, la pédagogie ne s'arrête pas à un stage de quelques jours.

Ainsi en vous inscrivant à une formation Clever-Institut, vous bénéficiez de l'ouverture d'un compte sur notre site internet vous permettant de :

- **exprimer, en amont du stage, vos attentes quant à cette formation, afin de nous permettre de personnaliser chacune de nos sessions**
- **déjeuner avec le formateur et les autres stagiaires, afin de transformer ce moment en partage et retours d'expérience**
- **évaluer la formation sur son contenu et sa pédagogie, et en partager le contenu avec les futurs stagiaires**
- **échanger avec votre formateur pendant les 15 jours qui suivent votre stage, pour toute question ou interrogation en rapport avec formation**

Comment s'inscrire ?

La demande d'inscription à une session de formation **se fait en ligne.**

Une fois votre inscription enregistrée, vous recevez dans les 48heures la Convention de Formation Professionnelle Continue simplifiée. Dès réception par nos services, de la convention signée, la convocation de stage est envoyée par mail aux stagiaires qui se voient ouvrir un compte sur notre site internet, leur permettant de préparer leur formation (accès, communication de leurs attentes, etc.).

A noter, que l'inscription est considérée comme définitve, à la signature de la convention de stage.