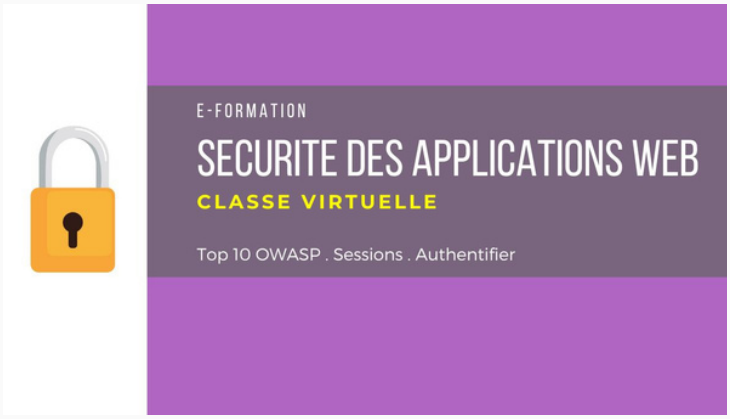
Module : Sécurité des applications web

L'objectif de ce module est d'apprendre à détecter les attaques et sécuriser les applications Web. Vous serez notamment capables de : connaître les différentes attaques et s'en prémunir, sécuriser les accès et les sessions, mettre en oeuvre les bonnes pratiques en matière de sécurité web.

Pré-requis : Web, langages de programmation.



Modalité : Classe virtuelle

Plateforme LIVE : ZOOM ou Teams

Durée totale : 21 H (3 jours)

Tarif € : 1898 €

Suivre cette formation en VOD (e-learning) ou en Streaming vidéo ?
Allez sur : www.reconvert.net

Sécuriser les applications Web : #5

Re-post des données
Timeout et déconnexion. Masquer les URL
Validation des données
Cookies et certificats numériques
Session ID et jeton de transaction
Vol de session (MITM proxy). Détournement
XSS ou Cross Site Scripting
Utilisation des références directes
CSRF (Token anti-CSRF). Sécurité d'accès au SGBD
SQL / Code Injection. Utilisation du JavaScript
Échapper des tags HTML
Authentification avec captcha
Attaques de force brute : cewl + Cupp.py
Mots de passe : salage, etc. Contrôle d'accès, privilèges
Sécuriser un upload de fichier

PLAN DETAILLE

Introduction : #1

Panorama de la sécurité Web
Terminologie, normes et lois
Les groupes de réflexions
Typologie WASC des menaces
Top 10 OWASP des menaces

Protocole HTTP : #2

Client / serveur
Ajax et DOM
Les headers HTTP
Les status code. Les méthodes HTTP
Ouverture sur Burp Suite

Vulnérabilités des applications Web : #3

Injections : SQL, LDAP, code...
Protection d'URL. Faille de référence
Stockage non sécurisé. Cross Site Scripting (XSS)
Session et authentification
Exposition de données sensibles
Attaque CSRF. Phishing.
Failles sur les configurations
Attaques de type DDOS
Désérialisation non sécurisée
Composants vulnérables
Analyse de site avec l'outil OWASP ZAP

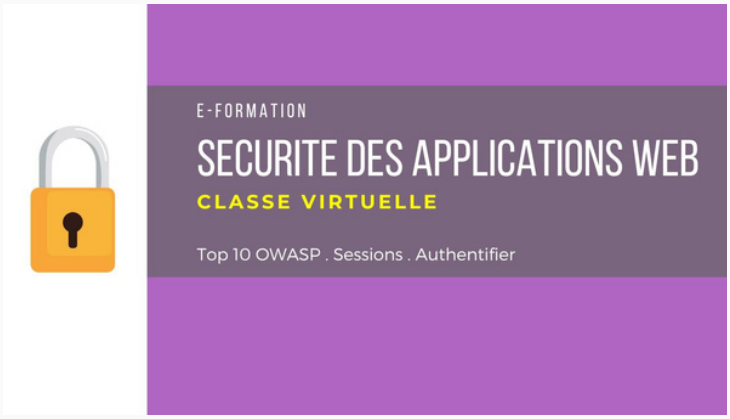
Technologies liées à la sécurité : #4

Firewalls: outils, techniques
Filtres des requêtes HTTP.
Empreinte de message
Algorithmes SHA-x et MD5
Signature numérique. Clé publique/ clé privée
Coffre à clé et coffre de confiance
Autorités de certification. Chiffrement de données
Algorithmes AES et RSA. Protocoles SSL, TLS
PKI, certificats X509. Authentification HTTP
Authentification par certificat. Analyseur de trame réseau
Proxy d'analyse HTTP

Module : Sécurité des applications web

L'objectif de ce module est d'apprendre à détecter les attaques et sécuriser les applications Web. Vous serez notamment capables de : connaître les différentes attaques et s'en prémunir, sécuriser les accès et les sessions, mettre en oeuvre les bonnes pratiques en matière de sécurité web.

Pré-requis : Web, langages de programmation.



Modalité : Classe virtuelle

Plateforme LIVE : ZOOM ou Teams

Durée totale : 21 H (3 jours)

Tarif € : 1898 €

Suivre cette formation en VOD (e-learning) ou en Streaming vidéo ?
Allez sur : www.reconvert.net

PLAN DETAILLE

Sécuriser les services Web : #6

SOAP, REST, gRPC
Authentification
Autorisation
Confidentialité et intégrité
Sécurisation : OAUTH, SAML, Token
Web Services Security

Contrôler la sécurité des applications Web : #7

Test d'intrusion, Burp suite
Audit de sécurité
Scanners de vulnérabilités
Veille technologique efficace
Déclaration des incidents de sécurité
Appareils mobiles : menaces et risques
Outils de piratage des mobiles
Mobiles : sécurisation