Sécurité des développements Web niveau 1 (BV-CASD1), certification Bureau Veritas

Cours Pratique de 5 jours - 35h
Réf : SDW - Prix 2024 : 3 830€ HT

Aujourd'hui quasiment tout est connecté et contrôlé via une application web, mobile ou non. Le développement web nécessite une maîtrise des techniques, des méthodologies et des moyens de sécurisation. Cette certification valide un socle de compétences et savoir pour aborder efficacement le développement sécurisé.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Identifier les vulnérabilités les plus courantes des applications Web

Comprendre le déroulement d'une attaque

Tester la sécurité de ses applications Web

Configurer un serveur Web pour chiffrer le trafic avec HTTPS

Mettre en place des mesures de sécurisation simples pour les applications Web

CERTIFICATION

Bureau Veritas Certification assure l'examen final de cette formation, délivrée par un organisme indépendant. Cet examen permet d'obtenir une certification de personne. Examen de 3 heures en 3 parties, sur une plateforme à distance : QCM, mise en situation sur points spécifiques, et sur cas concrets. Accès au support de cours et aux travaux pratiques pendant 3 semaines à compter du début de session. Passage de la certification en ce laps de temps. En cas d'échec, possibilité d'un second passage dans les 15 jours suivants le premier. Cette certification s'inscrit dans un schéma de certification visant à valider les savoirs requis pour les fiches métiers de l'ANSSI suivantes : spécialiste en développement sécurisé, auditeur de sécurité technique, développeur de solutions de sécurité, consultant en cybersécurité, formateur en cybersécurité, responsable de projet de sécurité.

PARTENARIAT

La certification est délivrée par Bureau Veritas Certification.
ORSYS et Bureau Veritas Certification se sont associés pour construire une offre de certifications couvrant les principaux domaines de la cybersécurité : architectures sécurisées, sécurité offensive et défensive, sécurité organisationnelle et système de management.

LE PROGRAMME

dernière mise à jour : 03/2022

1) Introduction

- Présentation des normes et efforts de standardisation.

PARTICIPANTS

Administrateurs réseaux, systèmes, Webmaster, auditeurs sécurité, chefs de projet développement sécurité.

PRÉREQUIS

Connaissances de base en systèmes, réseaux et Internet. Maitriser les fondamentaux de la programmation, connaitre un langage de programmation.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Importance de la sécurité du développement.
- RGPD et sécurité du développement.
- Security by design.
- Security by default.
- Les acteurs.

Travaux pratiques : Quiz.

2) Méthodologies

- Principes SecDevOps.
- Architectures associées.
- DREAD et STRIDE.
- SSDLC.
- BSSIM.
- OWASP.
- Analyse de risques.

Travaux pratiques : Réalisation d'une analyse de risques.

3) Compréhension des vulnérabilités et exploitations associées

- Typologie des menaces, le top 10 OWASP.
- Failles applicatives.
- Attaques côté client.
- Gestion de session et authentification.
- Failles de configuration.
- Attaques de type DDOS.
- Attaque Buffer-Overflow, XXE.

Travaux pratiques : Etude du top 10 OWASP.

4) Sécuriser son architecture

- Firewalls n-tier.
- Filtres de requêtes HTTP.
- Rappels algorithmique.
- Autorités de certification.
- Chiffrement de données.
- Protocoles.

Travaux pratiques : Sécurisation d'un serveur, certificat, waf, authentification.

5) Sécuriser son code

- Protections basiques.
- Usurpation d'identité.
- Se protéger des attaques client.
- Se protéger contre CSRF.
- Sécurité d'accès au SGBD.
- Protections contre les attaques de force brute.
- Liste de contrôle d'accès.
- Cheat cheat.

Travaux pratiques : Protection d'un code vulnérable.

6) Audits et tests de sécurité

- Les types d'audits.
- Tester la robustesse.
- Apprendre à connaitre son architecture.
- Organiser une veille technologique.
- Tests statiques vs tests dynamiques.

Travaux pratiques : Exercice d'audit, étude de rapports d'audit.

7) Vue sur la sécurité des applications mobiles

- Composants et contexte.

- Taxonomie des risques.
- Les principales menaces et attaques.
- Principes de sécurisation.

Travaux pratiques : Attaque sur une application Android.

8) Examen

- Révisions, examen blanc.
- Exaamen.

LES DATES

CLASSE À DISTANCE
2024 : 11 mars, 24 juin, 30 sept., 02 déc.

PARIS
2024 : 04 mars, 17 juin, 23 sept., 25 nov.