PHP, sécuriser ses applications
Pour les versions 8, 7 et 5

Cours Pratique de 3 jours - 21h
Réf : PSE - Prix 2024 : 2 070€ HT

De par sa nature même, le service dynamique de pages Web ouvre de nombreuses portes sur le monde extérieur. Pour le développeur, il est primordial de prendre conscience des types d'attaques auxquelles son code sera potentiellement exposé et de savoir y faire face, double objectif de ce stage.

OBJECTIFS PÉDAGOGIQUES

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

Prendre conscience des types d'attaques auxquelles son code peut être exposé

Intégrer la sécurité dans les développements dès la conception

Identifier les failles possibles au niveau des développements

Développer des applications plus sécurisées

MÉTHODES PÉDAGOGIQUES

Pédagogie active basée sur des exemples, des démonstrations, des partages d'expériences, des cas pratiques et une évaluation des acquis tout au long de la formation.

TRAVAUX PRATIQUES

Des postes sous Windows équipés des serveurs Apache2 avec PHP, MySql, Oracle, LDAP, FTP et mail seront mises à la disposition des participants.

PARTICIPANTS

Développeurs désirant développer des applications PHP plus sécurisées.

PRÉREQUIS

Bonnes connaissances des langages PHP et SQL. Connaissances de base de JavaScript.

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.

LE PROGRAMME

dernière mise à jour : 04/2022

1) Introduction

- Présentation des risques.
- Destruction de données.
- Détournement de site.
- Publication de données confidentielles.
- Abus de ressources.
- Vol d'identité.
- Plan Sécurité : Conception, Développement et Maintenance.

2) Les pages Web

- XSS principe et méthodes de protection. Moteur de recherche.
- CSRF : principe et contre-mesures. Virus en base de données.

3) Formulaires : la grande porte

- Les failles. Validation et limitations de l'approche JavaScript. Chaînage, attaques HTTP et Ajax. Contre-mesures.
- Validation des entrées. Tests et principe des listes. Expressions régulières, standards et filtres.
- Upload. Failles et contre-mesures.

4) Cookies et sessions

- Cookies. Principes et risques. Manipulation JavaScript. Tableaux de cookies.
- Sessions. Mode Cookie vs. Header. Principe du vol de session.

5) Sécuriser PHP : les bons réglages

- PHP.ini. Directives sensibles, sessions et erreurs.
- Protéger les scripts. Protection physique. Exécution de scripts distants ou à la volée.

6) Bases de données

- Failles potentielles. Administration. Stockage.
- Injections SQL. Principe et contre-mesure. Procédures stockées et requêtes paramétrées. Limites.
- Fichiers d'accès. Organisation et valeurs par défaut. Accès anonymes et protocoles.

7) Sécuriser l'emploi des extensions

- Email. Spam via un formulaire de contact : injections et contre-mesures.
- Accès réseau par PHP. Appels séquentiels et récursifs. Attaque furtive.

8) Considérations générales

- BFA. Principe. Identification et contre-mesures.
- Phishing. Principe et formation des utilisateurs.
- DoS. Quotas et gestion des charges.
- Mots de passe. Renforcement et stockage. .
- Chiffrement et signature. Cryptage / décryptage : implémentation PHP et MySQL.
- Ruses. Pot de Miel, Obfuscation et Turing inversé.
- Frameworks et briques logicielles. Gestion de la sécurité dans les développements composites.
- Audit de sécurité. Méthodologie de base, Cross-test et rapport d'audit.

LES DATES

CLASSE À DISTANCE
2024 : 17 juil., 07 oct.

PARIS
2024 : 10 juil., 30 sept.