DOCAPOSTE Institute

Sécurité applicative avec PHP

Présentation

Cette formation aborde les vulnérabilités du Web, à travers des exemples basés sur PHP, allant au-delà du top dix de l'OWASP, en abordant diverses attaques par injection, des injections de script, des attaques contre la gestion des sessions de PHP, des références directes d'objets non sécurisées, des problèmes de téléchargement de fichiers, et bien d'autres.

Cette formation sur la sécurité applicative PHP vous permettra de maîtriser les techniques et les fonctions les plus importantes à utiliser pour atténuer les risques encourus.

Durée : 21,00 heures (3 jours)
Tarif INTRA : Nous consulter

Objectifs de la formation

- Comprendre les concepts de base de la sécurité, de la sécurité informatique et du développement sécurisé
- Apprendre les vulnérabilités du Web au-delà du Top 10 de l'OWASP et savoir comment les éviter
- Apprendre à utiliser les différentes fonctions de sécurité de PHP
- Obtenir des informations sur certaines vulnérabilités récentes des frameworks PHP (celui que chacun utilise)
- Découvrir les erreurs de code typiques et comment les éviter
- Acquérir des connaissances pratiques sur l'utilisation des outils de test de sécurité
- Obtenir des sources et des lectures complémentaires sur les pratiques de développement sûres

Prérequis

- Connaissances en programmation Web

Public

- Développeurs

Docaposte Institute
45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE France
Tél : 01 56 29 70 01 - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

- Architectes
- Testeurs de sites Web

Programme de la formation

Sécurité informatique et développement sécurisé

- Nature de la sécurité
- Termes liés à la sécurité informatique
- Définition du risque
- Les différents aspects de la sécurité informatique
- Exigences des différents domaines d'application
- Sécurité informatique vs. Développement sécurisé
- Des vulnérabilités aux botnets et à la cybercriminalité
- Classification des failles de sécurité

Vulnérabilités des applications web

- OWASP Top 10 - 2017
  - A1 - Injection
  - A2 - Authentification cassé et gestion de session
  - A3 - Scripting cross-site (XSS)
  - A4 - Contrôle d'accès cassé
  - A5 - Mauvaise configuration de la sécurité
  - A6 - Exposition aux données sensibles
  - A7 - Protection insuffisante contre les attaques
  - A8 - Falsification des demandes intersites (CSRF)
  - A9 - Utilisation de composants présentant des vulnérabilités connues
  - A10 - API sous-protégées

Les bases de la cryptographie

- Crypto-systèmes
- Cryptographie à clé symétrique
- Autres algorithmes cryptographiques
- Cryptographie asymétrique (à clé publique)
- Infrastructure à clés publiques (PKI)

Sécurité côté client

- Sécurité JavaScript
- Sécurité Ajax

Docaposte Institute
45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE France
Tél : 01 56 29 70 01 - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

- Sécurité HTML5

Services de sécurité PHP
- Modules de cryptographie en PHP
- APIs de validation des entrées

Environnement PHP
- Configuration du serveur
- Sécuriser la configuration PHP
- Sécurité de l'environnement
- Durcissement
- Gestion de la configuration

Conseils et principes
- Les principes de Matt Bishop pour une programmation robuste
- Les principes de sécurité de Saltzer et Schroeder

Validation des entrées
- Concepts de validation des entrées
- Des sources d'informations sur le sujet
- Des sources d'informations sur le développement sûr
- Exécution de code PHP à distance
- Erreurs de validation MySQL - au-delà de l'injection SQL
- Erreurs de portée des variables en PHP
- Les spammeurs et les upload de fichiers
- Manipulation de l'environnement

Mauvaise utilisation des dispositifs de sécurité
- Problèmes liés à l'utilisation des dispositifs de sécurité
- Aléatoire non sécurisé
- Faiblesses des générateurs de nombres pseudo-aléatoires (PRNG) en PHP
- Des PRNGs plus sécurisés que nous pouvons utiliser en PHP
- Gestion et stockage des mots de passe
- Quelques problèmes habituels de gestion des mots de passe
- Stockage des identifiants pour les systèmes externes
- Violation de la vie privée
- Traitement incorrect des erreurs et des exceptions

Docaposte Institute
45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE France
Tél : 01 56 29 70 01 - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

Problèmes de temps et d'état

- Concurrence et threading
- Concurrence en PHP
- Prévenir les situations de compétition de fichiers
- Problème de double soumission/envoi
- Gestion des sessions PHP
- Un défaut de conception de PHP - situation de compétition open_basedir
- Les situations de compétitions des bases de données
- Possibilités de déni de service (DoS)
- Attaque par collision de tables de hachage

Utilisation des outils de test de sécurité

- Scanners de vulnérabilité web
- Outils d'injection SQL
- Base de données publique
- Piratage de Google
- Serveurs proxy et sniffers
- Capture du trafic réseau
- Analyse du code statique

Organisation

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes.

Moyens pédagogiques et techniques

- Apports didactiques pour apporter des connaissances communes.
- Mises en situation de réflexion sur le thème du stage et des cas concrets.
- Méthodologie d'apprentissage attractive, interactive et participative.
- Equilibre théorie / pratique : 60 % / 40 %.
- Supports de cours fournis au format papier et/ou numérique.

Docaposte Institute
45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE France
Tél : 01 56 29 70 01 - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

- Ressources documentaires en ligne et références mises à disposition par le formateur.
- Pour les formations en présentiel dans les locaux de Softeam, les stagiaires sont accueillis dans une salle de cours équipée d'un réseau Wi-Fi, d'un tableau blanc ou paperboard. Un carnet de notes est offert. Un ordinateur avec les logiciels appropriés est mis à disposition (le cas échéant).

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation :

- Recueil des besoins : permet de récolter des informations sur le stagiaire (profil, formation, attentes particulières, ...).
- Auto-positionnement des stagiaires afin de mesurer le niveau de départ.

Tout au long de la formation :

- Évaluation continue des acquis via des questions orales, exercices / projet fil rouge, des QCM, des cas pratiques et mises en situation.

A la fin de la formation :

- Auto-positionnement des stagiaires afin de mesurer l'acquisition des compétences.
- Evaluation du formateur des compétences acquises par les stagiaires.
- Questionnaire de satisfaction à chaud : permet de connaître le ressenti des stagiaires à l'issue de la formation.
- Questionnaire de satisfaction à froid : permet d'évaluer les apports réels de la formation et leurs mises en application au quotidien.

Accessibilité

Cette formation est **accessible** aux personnes en situation de handicap, consultez-nous pour plus d'informations.

Docaposte Institute
45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE France
Tél : 01 56 29 70 01 - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France