

PHP Sécurité

Objectif :

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.

Cette formation PHP sécurité se concentre sur le point de vue du développeur, les aspects "sécurisation serveur" étant abordés dans les cours d'administration.

Une approche pratique basée sur des sessions de hacking éthique.

Participants :

Cette formation s'adresse aux développeurs PHP ayant déjà une bonne pratique du langage, désirant développer des applications sécurisées.

Pré-requis :

Les participants doivent bien connaître la programmation sous PHP / Sql et avoir de bonnes notions de programmation Client (javascript).

Travaux pratiques :

Des machines sous windows XPPro équipées des serveurs Apache2 avec PHP5, MySql, Oracle, LDAP et mail seront mis à la disposition des participants.

Durée : 3 jours (21 heures) Référence : IPHS

Contenu de la formation :

Comprendre pour réduire les risques des applications PHP.

Les Risques

- Destruction de données
- Détournement de site
- Publication de données confidentielles
- Abus de ressources
- Vol d'identité

Plan Sécurité

- Conception, Développement et Maintenance

Sécurité et Pages Web.

XSS

- Principe et méthodes de protection
- moteur de recherche

ATELIER

Mise en oeuvre et contrage d'une injection sur le site BDPhilia.

CSRF

principe et contre-mesures
virus en base de données

ATELIER

Mise en oeuvre d'une propagation sur le forum BDPhilia .

Formulaires PHP: 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

ATELIER

Exécution maligne d'un fichier téléchargé via le backoffice de BDPhilia..

Sécurité PHP : Cookies et Sessions

Cookies

Principes et risques.
Manipulation Javascript
Tableaux de cookies.

Sessions

Mode Cookie vs. Header
Principe du vol de session.

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

ATELIER

Réglage des options sensibles. Discussion sur les conséquences au niveau développement.

Sécurité PHP : Bases de Données

Failles potentielles.

risques : données et 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

ATELIER

Utiliser la pagination du moteur de recherche BDPHilia pour modifier des données et des droits.

Sécuriser l'emploi des extensions en PHP.

Se protéger contre le SPAM.

Spam via un formulaire de contact : Injections et contre-mesures

ATELIER

Utiliser un formulaire de contact pour envoyer un mail à 3 adresses différentes.

Accès réseau par PHP.

Appels séquentiels et récursifs
Attaque furtive.

ATELIER

Soumettre une url détournée.

La boîte à outils.

BFA.

Principe : Dictionnaire
Identification et Contre-mesures.

ATELIER

Mise en oeuvre des outils nécessaires à une BFA.

Phishing.

Principe et Formation des utilisateurs.

ATELIER

Analyse de différents cas, identification des victimes potentielles.

DoS

Quotas et gestion des charges.

ATELIER

Mise en oeuvre d'une file d'attente pour la génération graphique de T-Shirts sur BDPhilia.

Mots de Passe.

Renforcement et stockage
Création et rappel

ATELIER

Mise en oeuvre d'une inscription sécurisée pour l'espace client de BDPhilia.

Chiffrement et Signature.

Cryptage / décryptage : Implémentation PHP et MySQL.

ATELIER

Cryptage des données client.

Ruses de Sioux.

Pot de Miel, Obfuscation et Turing inversé.

ATELIER

Créer un pot de miel pour l'admin du BO, obfusquer les formulaires de recherche en MD5 et appliquer un test de Turing inversé sur le formulaire de contact.

Frameworks et briques logicielles.

Gestion de la sécurité dans les développements composites

Audit de Sécurité.

Méthodologie de base, Cross-test et Rapport d'Audit.

ATELIER

Rédigez un rapport d'audit sur la version de base de BDPhilia, et sur les mesures prises pour améliorer la situation.