PHP Sécurité - Formations - Seeren

Formation

Durée: 3 jours
Objectif: Sécuriser une application web, identifier et exploiter des failles de sécurité.
Public: La formation s'adresse à un public déjà initié, développeurs, intégrateurs ou chef de projet souhaitant renforcer leurs connaissances du thème sécurité des applications web. Plus généralement à tout public intéressé par le pentesting et les problématiques liés au web.
Prérequis: Les stagiaires doivent être initiés à PHP et JavaScript. Il reste possible de suivre cette formation sans ces notions à condition d'avoir des connaissances sur un autre langage de programmation web.

Programme

Injection SQL

Présentation
Base de données
Scénario
Injections
Protections

Violation de Session

Présentation
Configuration
Scénario
Fixation par SID
Fixation par XSS
Prédiction
Protections

Cross-Site Scripting (XSS)

Présentation
DOM Based
Reflected
Stored
Protections

Référence directe à un objet sécurisé

Présentation
Table
Scénario
Broken Access
Access Map
Protections

Mauvaise configuration de Sécurité

Présentation
Privilèges

Directives
Erreurs

Exposition de données sensibles

Présentation
Scénario
Casser un hachage
Cryptage symétrique
Crypter AJAX
Protections

Manque de contrôle d'accès au niveau fonctionnel

Présentation
Directory traversal
Force browsing
Ressources
Protections

Falsification de requête intersite (CSRF)

Présentation
Configuration
Forgerie
Itération
Protections

Utilisation de composants vulnérables

Présentation
Symfony
Cake
WordPress
Joomla
Protections

Redirections et Renvois Non Validés

Présentation
Scénario
Contrefaçon
Protections

Téléchargement de fichiers sans restriction

Présentation
Scénario
Exploitation
Protections

Open Web Application Security Project

Testing Guide
Code Review
WebGoat
Zed Attack Proxy Project