

## Programme de formation

### WordPress Sécurité

Sécuriser ses développements WordPress, de la détection des failles à la maîtrise des plugins, vous apprendrez à sécuriser entièrement un site web WordPress

#### Durée

1 jour / 7 heures

#### Description

Cette formation Sécurité avec WordPress vise à sécuriser ses développements sous WordPress, détecter les failles et ajouter de la sécurité dans un projet.

Toutes les bonnes pratiques de développement orientées sécurité seront abordées. Le formateur Wordpress mettra en évidence la vigilance particulière à apporter aux plugins, comment choisir un plugin & un thème sécurisé et s'assurer que le site ne se fera pas piraté dans la semaine de lancement.

#### Objectifs pédagogiques

- Appréhender les failles d'un site web sous WordPress
- Sécuriser les développements liés au site WordPress
- Eviter le piratage de son site web Wordpress

#### Public

Développeurs PHP, Architectes

#### Pré-requis

Développement PHP, WordPress et Html/Css, connaissance des bases de Apache/htaccess

#### Méthodes pédagogiques

50 % théorie / 50 % pratique

#### Profil intervenant

L'ensemble de nos formations sont animées par des formateurs expérimentés possédant une expérience terrain éprouvée.

#### Modalités d'évaluation

L'évaluation des acquis se fait tout au long de la session au travers d'ateliers de mise en pratique des notions et concepts abordés pendant la formation.

## Programme

### Introduction à la sécurité d'un site sous WordPress

- Pourquoi votre site est-il pris pour cible ? Pourquoi cibler WordPress ?
- Les mécanismes de réflexions des attaquants
- Sachez réfléchir, naviguer comme eux, devenez attaquant !

### Installation de WordPress

- Installation de WordPress en local sous XAMPP
- Configuration avancée des fichiers wp-config.php, .htaccess et robots.txt

### Retour sur les paramètres de l'administration

- Oubliez et réapprenez les menus avec un oeil sécuritaire
- L'éditeur de fichier, oui ou non ? Pourquoi ?

### Aidez-vous et WordPress vous aidera

- Connaissez toutes les fonctions WordPress dédiées à la sécurité
- Les données utilisateurs : Filtrer ? Désinfecter ? Bloquer ? Comment choisir ?
- Apprenez les bons gestes qui sauvent vos développements

### Les failles web

- Connaissez et reconnaissez les failles les plus répandues
- Comment corriger chacune de ces failles dans votre plugin
- Détectez les failles dans les plugins d'autres auteurs

### Le contenu de WordPress

- Quels fichiers sont importants, pourquoi ?
- Comment envoyer des fichiers, ajouter des plugins et thèmes de façon sécuritaire
- Navigation SSL ? Navigation Privée ?

### Les plugins

- Le minimum fait le maximum : quels plugins utiliser, dans quels cas ?
- Développez vos propres plugins : écoutez vos besoins afin d'être sécurisé,
- Re développez vos anciens plugins, tenez vous à jour !

### Les thèmes

- Attention aux thèmes gratuits malicieux, comment les reconnaître ?
- Comment corriger ces codes malicieux ?

### Votre quotidien en tant qu'administrateur WordPress

- Ne négligez pas votre ordinateur ni votre navigateur
- Évitez l'ingénierie sociale

### Comment se sortir d'un piratage ?

- Trouvez le pourquoi et comment de ce piratage
- Que faire ensuite ? Ou trouver les ressources ?

Comment éviter le retour de flammes ?