CMS : Wordpress

CMS - Wordpress introduction

Wordpress est un CMS, càd un système de gestion de contenu (de l'anglais Content Management System). Un CMS permet de concevoir et de mettre à jour un site internet dynamique.

Wordpress est devenu le CMS le plus populaire, particulièrement dans les petites entreprises. Mais Wordpress est aussi le CMS qui fait l'objet de nombreuses attaques par les hackers. Il est donc très important de le sécuriser.

Voir enquête de Smile : http://www.smile.fr/Ressources/Livres-blancs/Gestion-de-contenu-et-ged/Enquete-cms

Les principaux CMS opensource du marché

Wordpress : http://fr.wordpress.org/
basé sur PHP/MySQL

Joomla : http://www.joomla.fr/
basé sur PHP/MySQL (architecture MVC)

Drupal : https://drupal.org/
basé sur PHP/MySQL

Spip : http://www.spip.net/
basé sur PHP/MySQL

Typo 3 : http://typo3.org/
basé sur PHP/MySQL, full HTML5

EzPublish : http://ez.no/fr/
basé sur PHP et MySQL

CMS Made Simple : http://www.cmsmadesimple.fr/
basé sur PHP et Smarty

Jahia : http://www.jahia.com/fr/
Excellent produit, basé entre autre sur Java

Liferay : http://www.liferay.com/fr
basé sur J2EE

Plone : http://plone.org/
basé sur Python

Les CMS spécifiques au e-commerce

Prestashop : http://www.prestashop.com/fr/
basé sur PHP/MySQL et Smarty

Magento : http://magento.com/
basé sur PHP/MySQL

Thelia : http://thelia.net/
basé sur le framework PHP Symfony 2 et Smarty

Oscommerce : http://www.oscommerce.com/

Avantages des CMS

- Ce sont des solutions documentées et standardisées.
- La mise en ligne d'un site est rapide et facile, sans ou avec peu de programmation => gains au niveau des temps et des coûts de développement.
- De nombreux modules sont disponibles, gratuitement ou à faible coût.
- Il existe des communautés d'utilisateurs et de développeurs.
- Les mises à jour sont fréquentes : corrections des failles de sécurité, des bogues.

Inconvénients des CMS

- Principalement des problèmes de sécurité : l'emplacement du panneau administrateur est connu de tous, certains plugins peuvent comporter des scripts pour hacker le site.
- Les failles de sécurité sont connues et exploitées par les hackers => Il faut impérativement prévoir un contrat de maintenance pour les mises à jour.
- C'est une boîte noire dans laquelle il est plus complexe d'intervenir.
- Le site est plus lourd à charger.
- La migration de version est parfois complexe (par exemple entre Joomla 1.5 et Joomla 2.5).

Installation de Wordpress

Sur un ordinateur personnel : installation d'un serveur WAMP (PC), MAMP (MAC), LAMP (Linux) ou XAMPP (multi-plateformes).

Chez un hébergeur web : vérifier si l'hébergeur accepte le PHP et les bases de données en MySQL (c'est le cas de la plupart des hébergeurs).

L'hébergeur doit aussi accepter la réécriture d'URL (sinon impact négatif sur le référencement).

Sur les hébergements mutualisés, le CMS est souvent préinstallé, sinon il faudra transférer les sources via un client FTP comme FileZilla et créer la base de données avec phpMyAdmin.

Sur l'ordinateur personnel, il sera généralement nécessaire de lancer manuellement le serveur PHP (Wamp Server, MAMP, XAMPP).

Sur les ordinateurs de la 3W Academy, le serveur PHP tourne déjà.

Création de la base de données

Pour créer la base de données, on va se connecter à phpMyAdmin : http://localhost/phpmyadmin

Création d'un utilisateur dont les accès seront limités au Wordpress qu'on va installer (onglet utilisateur). Sur un hébergement mutualisé, cette procédure se fait généralement via l'hébergeur et non via phpmyadmin.

Compléter les champs :

- Nom d'utilisateur : identifiant, sans espaces, ni caractères spéciaux
- Client : localhost
- Mot de passe : pour le localhost, la sécurité ne doit pas être élevée. Sur un hébergement, il est conseillé d'utiliser un générateur de mot de passe aléatoire.

- Dans base de données pour cet utilisateur : cocher la case "Créer une base portant son nom et donner à cet utilisateur tous les privilèges sur cette base".
- Cocher la case « Tous les privilèges »
- Cliquer sur le bouton "Créer un utilisateur"

La base de données est à présent créée et on va pouvoir installer Wordpress

Transfert des sources

Aller sur le site https://fr.wordpress.org/ pour télécharger la dernière version de Wordpress en français ou sur https://wordpress.org/download/ pour la dernière version en anglais.

Ne pas utiliser d'anciennes versions.

Décompresser l'archive.

- Sur Ubuntu, copier l'archive décompressée dans le dossier sites.
- Sur PC => C://wamp/www (Wampserver) ou c://xampp/htdocs (xampp)
- Sur MAC => /Applications/MAMP/htdocs (Mamp) ou /Applications/xampp/htdocs
- Sur un hébergement, transférer les sources avec un client FTP

Lancer l'installation

Aller sur localhost/wordpress (ou le nom du répertoire que vous avez créé) ou sur l'URL de votre hébergement.

Wordpress vous redirige sur l'URL wp-admin/setup-config.php => cliquer sur "C'est parti"

La page suivante vous demande les informations concernant la base de données.

- Nom de la base de données : le nom que vous avez choisi lors de la création de l'utilisateur
- Identifiant : le nom de l'utilisateur BD (<> de celui de l'administrateur du back-office)
- Mot de passe : mot de passe de l'utilisation BD
- Adresse de la base de données : localhost (ou le paramétrage de votre hébergeur)
- Préfixe des tables : par mesure de sécurité, il est très fortement recommandé de ne pas laisser le préfixe "wp_" que l'installateur de Wordpress vous propose. Il est conseillé de choisir un préfixe plus long (5 caractères, avec des lettres minuscules + 1 ou 2 chiffres) choisi de manière aléatoire. En cas de tentative de piratage d'un site, le hacker va d'abord tenter d'utiliser le préfixe wp_, autant ne pas lui faciliter la tâche. Même s'il est possible par la suite de renommer les tables, c'est une opération délicate car le 'wp_' est utilisé à de nombreux endroits dans les tables Wordpress et il faut bien s'y connaître pour effectuer ce type de manipulations.
- Cliquez sur "Valider"

Ensuite, on va introduire les données du site

- Titre du site : Mindgeek (peut être modifié ultérieurement)
- Identifiant : par mesure de sécurité, ne jamais utiliser admin. C'est ce mot clé qui est le plus souvent utilisé par les hackers et les robots lors d'attaques de type "brute force". Eviter aussi webmaster, administrateur et toute info qui peut être aisément trouvée. A noter que par défaut, Wordpress ne permet pas de modifier l'identifiant par la suite,

mais un administrateur Wordpress peut toutefois y parvenir en allant modifier certaines informations dans les tables MySQL.

Par défaut, Wordpress propose désormais un mot de passe aléatoire fort qu'il convient de noter. En localhost, on peut toutefois utiliser un mot de passe faible, mais il faudra impérativement le modifier avant la mise en ligne du site.

- Cliquer sur "Installer Wordpress" et voilà le site est prêt à être utilisé.

Structure d'un site Wordpress

wp-config.php : fichier de configuration

wp-content : contenu de Wordpress, contient 3 sous-dossiers : themes (templates), plugins (extensions), languages (langues) et uploads (médias)

wp-admin : administration de Wordpress

wp-includes : le coeur de Wordpress

Quelques extensions utiles

Yoast SEO : indispensable pour le référencement

Remove Author Pages : indispensable pour sécuriser Wordpress, car par défaut le CMS publie un plan des auteurs de pages, et donc des identifiants des administrateurs

WP-reCAPTCHA : sécurisation des formulaires

Page builder by Site Origin : permet une mise en page aisée et souple, sans devoir coder. Il peut s'installer sur tous les templates modernes.

AddToAny Share Buttons : boutons de partage du contenu sur les réseaux sociaux

WP Cerber : protection contre les attaques de type brute force

Contact Form 7 : formulaire de contact

WooCommerce : pour faire un site marchand

Sécuriser Wordpress

- Limiter le nombre d'administrateurs
- Pour les clients, préférer le niveau "Editeur"
- Désinstaller les thèmes et les extensions qui ne sont pas utilisés (via l'interface)
- Supprimer l'affichage de la balise meta generator (fichier functions.php)
- Modifier l'URL du back-office à l'aide d'un plugin
- Installer un captcha pour accéder à l'interface d'administration
- Faites régulièrement une sauvegarde du site et mettez votre version core de Wordpress ainsi que les extensions à jour.