WordPress

Sécurisation

Sources:

- https://korben.info/securiser-wordpress-installation.html
- https://www.b-website.com/installer-wordpress-dans-un-sous-repertoire
- http://www.geekpress.fr

Pré-installation

1. Créer une base de données avec un nom aléatoire
2. Créer un utilisateur pour cette BDD avec un nom aléatoire et un mot de passe robuste
3. Créer un répertoire sur l'hébergement avec un nom aléatoire (alphanumérique), nous y mettrons le contenu de wordpress

Installation

1. Préfixer les tables avec un aléatoire (alphanumérique) au lieu de wp_
2. Identifiant admin du site, un aléatoire et un mot de passe robuste
3. Adresse de messagerie: un aléatoire, un compte mail dédié au pire

Configuration

1. Changer url d'accès dans URL/ALEATOIRE/Réglages/Général/Réglages/Général/Adresse web du site (URL) et mettre l'url du domaine.
2. Rafraichir les permaliens dans URL/ALEATOIRE/Réglages/Général/Réglages/Permaliens en changeant le type d'url rewriting et enregistrer, puis faire la manipulation inverse.
3. Déplacer le fichier index.php à la racine du FTP et modifier la dernière ligne:

```
require('./ALEATOIRE/wp-blog-header.php');
```

Configuration utilisateurs

1. Décocher URL/Réglages/Général/Tout le monde peut s'enregistrer
2. Changer pseudonyme URL/Utilisateurs/Pseudonyme (nécessaire)
3. Le sélectionner dans URL/Utilisateurs/Nom à afficher publiquement

Toutefois, l'affichage de ce “nom public” ne sera effectif que si c'est ce que votre thème appelle comme variable. Vérifiez donc dans les pages de votre thème que c'est bien le

nom public qui est appelé avec la fonction suivante :

```
<?php the_author(); ?>
```

Mise à jour automatiques

Ajouter dans wp-config.php

```
define( 'WP_AUTO_UPDATE_CORE', 'minor' );
```

Éditeur de code

Pour le désactiver, ajouter dans wp-config.php

```
define('DISALLOW_FILE_EDIT',true);
```

Le fichier wp-config.php

Ce fichier contient, entre autres, les clés de sécurité, qui dont celles de l'installation par défaut.

```
/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link
https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key
service}
 * You can change these at any point in time to invalidate all existing
cookies. This will force all users to have to log in again.
 *
 * @since 2.6.0
 */
```

Nous allons les modifier via l'outil spécifié https://api.wordpress.org/secret-key/1.1/salt/
On verrouille l'accès au fichier ainsi qu'au *.htaccess*:

```
<Files .htaccess>
   order allow,deny
   deny from all
</Files>
```

```
<Files wp-config.php>
   order allow,deny
   deny from all
</Files>
```

Et les droits d'accès

```
chmod 644 wp-config.php
chmod 644 .htaccess
```

Modifications dans le thème

Message d'erreur login trop bavard

Pour changer le message d'erreur de la page login, ajouter dans le fichier functions.php du thème la ligne suivante:

```
add_filter('login_errors', create_function('$no_login_error', "return
'Mauvais identifiants';"));
```

Par défaut c'est le thème Twenty Seventeen

Cacher les numéros de version

```
remove_action('wp_head', 'wp_generator');
```

Les plugins

Passer par le store officiel...

Les thèmes

Prendre des thèmes ayant une bonne réputation, chez leurs auteurs, au mieux sur la forge de WordPress. Pour vérifier qu'un thème ne contienne pas de code malicieux ou des liens publicitaires qui seraient encodés en base64 (de la lecture) nous chercherons l'instruction *base64_decode*.
Sous GNU/Linux et/ou Mobaxterm Windows:

```
cd DOSSIER_THEME
grep -inHR base64_decode * | cut -d':' -f1,2
```

Sous windows:

```
cd DOSSIER_THEME
findstr /s /i base64_decode  *.*
```

En PHP:
Faire un for récursif sur les fichiers du thème et utiliser la fonction *preg_grep*:

1. plus long que en local
2. le serveur va vous faire la gueule

- php.ini : Il s'agit du fichier de configuration de PHP présent en général dans /etc./.
- wp-config.php : Il s'agit du fichier de configuration de WordPress qui contient entre autres des clés de chiffrement et les accès à la base de données
- .htaccess : Il s'agit de fichiers qui se placent à la racine des répertoires et qui permettent de configurer le comportement d'Apache pour ces répertoires spécifiques.