WordPress : fichier wp-config.php

Il s'agit du fichier de configuration qui est généré à l'installation de WordPress, il est situé à la racine de votre site web.

Il contient les informations sur la base de données et la définition d'options avancées.

Configuration des accès à la base de données

Vous retrouvez dans le fichier **wp-config.php** les identifiants de connexion à votre base de données.

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'local' );

/** MySQL database username */
define( 'DB_USER', 'root' );

/** MySQL database password */
define( 'DB_PASSWORD', 'root' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
```

- **DB_NAME :** nom de la base de données
- **DB_USER :** nom d'utilisateur pouvant se connecter à la base de données
- **DB_PASSWORD :** mot de passe associé à l'utilisateur
- **DB_HOST :** l'adresse du serveur où se situe la base de données (hébergement MySQL)
- **DB_CHARSET :** jeu de caractères / encodage (**utf8** recommandé pour prendre en compte tous les caractères non latins)

Le préfixe des tables

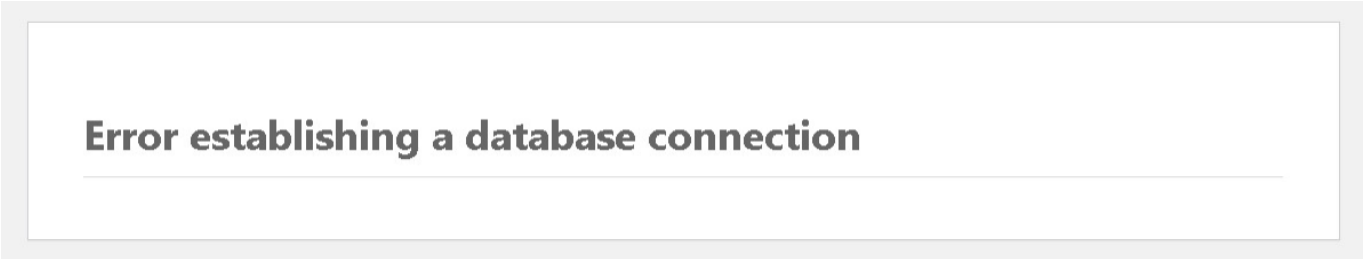
Le préfixe des tables de base de données est **une chaîne de caractères utilisée pour préfixer tous les noms de table** créés par WordPress lors de l'installation du système.

Par défaut, le préfixe des tables de base de données de WordPress est généralement défini sur

« **wp_**« .

Erreur de connexion à la base de données

Une erreur dans le fichier wp-config.php ou un serveur de base de données HS :



Basculer son site WordPress en mode DEBUG

Le **mode de débogage** est un outil intégré qui permet d'identifier et de résoudre les erreurs et les problèmes rencontrés sur un site WordPress.

Lorsque le mode de débogage est activé, des informations détaillées sur les erreurs PHP, les avertissements et les notifications sont affichées, ce qui facilite le processus de débogage.

```
define('WP_DEBUG', true);
// Enregistrement des erreurs dans un fichier debug.log stocké dans /wp-content/
define('WP_DEBUG_LOG', true);
// Affichage à l'écran
define('WP_DEBUG_DISPLAY', true);
```

Activer le mode debug :

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

Lorsque **WP_DEBUG** est activé, WordPress affiche les erreurs, les avertissements et les notifications liés au développement (ex. fonctions dépréciées, variables non définies…).

Une fois le site basculé en production, n'oubliez pas de désactiver le mode de débogage pour éviter l'affichage disgracieux des erreurs, qui pourraient également être exploitées par les hackers.

Activer le mode debug dans le fichier /wp-content/debug.log :

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

Vous pouvez également définir précisément dans quel dossier vous souhaitez enregistrer le fichier de débogage.

```
define( 'WP_DEBUG_LOG', '/dossier/fichier' );
```

Astuce : il existe des extensions dédiées au débogage comme **Query Monitor** ou **Debug Bar** qui donnent accès à des informations supplémentaires (requêtes en base de données, hooks executés, styles et scripts chargés, …).

Environnement d’exécution

Depuis WordPress 5.5, plusieurs environnements différents peuvent être configurés :

- **development :** lorsque vous travaillez en local
- **staging :** lorsque vous basculez en préproduction
- **production**

L’environnement d’exécution peut être défini depuis le fichier **wp-config.php** au travers de la constante **WP_ENVIRONMENT_TYPE**.

```
// En mode 'development' WP_DEBUG est à true
define( 'WP_ENVIRONMENT_TYPE', 'development' );
```

Ces environnements vont vous permettre d’exécuter du code sous condition (ex. envoyer un mail uniquement en mode production), en récupérant le status via la fonction **wp_get_environment_type()** de WordPress.

```
<?php
    switch ( wp_get_environment_type() ) {
        case 'local':
        case 'development':
            echo "<span class=\"text-white\">MODE DEVELOPPEMENT</span>";
            break;

        case 'staging':
            /*do_staging_thing();*/
            break;

        case 'production':
        default:
            /*do_production_thing();*/
            break;
    }
?>
```

Clés de sécurité secrètes

Depuis WordPress 2.6 vous pouvez améliorer la sécurité de votre site web grâce à 4 clés de sécurité générées aléatoirement.

Les mots de passe stockés dans la base de données ne le sont pas « en clair », ils sont chiffrés.

Ce chiffrement utilise des clés uniques (**clés de salage**) stockées dans le fichier **wp-config.php**.

Générateur de clés de salage

Un outil en ligne vous permet de les générer : https://api.wordpress.org/secret-key/1.1/salt/

```
define('AUTH_KEY',         'Tsk(ZbK5U$4Z.`Qq|lU yh0`p+C?#xQ0Cs+CK-7D~5q ,I;8&|r:IUq[`9dw|FX_');
define('SECURE_AUTH_KEY',  '[K)i+|=i)|w&@@(+SJEs@%7Y5d_XqB!;Aq:{={9a{{+1M=YEC=V(/8=_6Y/-TGp2');
define('LOGGED_IN_KEY',    '!R4/JaL+~VI:{<eCjCy,tU61)ie7ETU~fa)]9QU:[>hK@WIb*Pu2-J,SDl._riPu');
define('NONCE_KEY',        '%t*#q_eoG&:?XRuqQ1%WN:SZ8v2|W8DX)hEysQZVdlG0;iRJE80f8C1O%t-K1t<D');
define('AUTH_SALT',        '|y~h.)%nkO:}D;{L(#Fw1|<[z]f}rifJJIr e_cgvgW@Wj_j?*Q.<uZdhptz(Pi~');
define('SECURE_AUTH_SALT', '&$Ew0-i0@MEbV$?-A|s{&TWStea[*Ld;cO>`<Bs8&$+$jY9JaU1KpEgH~G~vsk*]');
define('LOGGED_IN_SALT',   '/KH?>_K_zr>NDFfU`DjBS#z3 1RH A_(H),6P-)_C(j*BpF1fG} w1P=~e621sPn');
define('NONCE_SALT',       '|Oih *!{!4a^~De7W](g~}Rn1;`$Kc|.Vf5%}--8naCP`v}FoaF+RGNvDE7^S<7|');
```

Huit clés de salage sont générées aléatoirement, chacune avec une utilité particulière.

Ex.

- **AUTH_KEY** pour l'authentification,
- **NONCE_KEY** pour les **nonces** qui sont utilisés pour vérifier la provenance des données d'entrée des formulaires et éviter les attaques de sécurité de type **XSS**),
- …

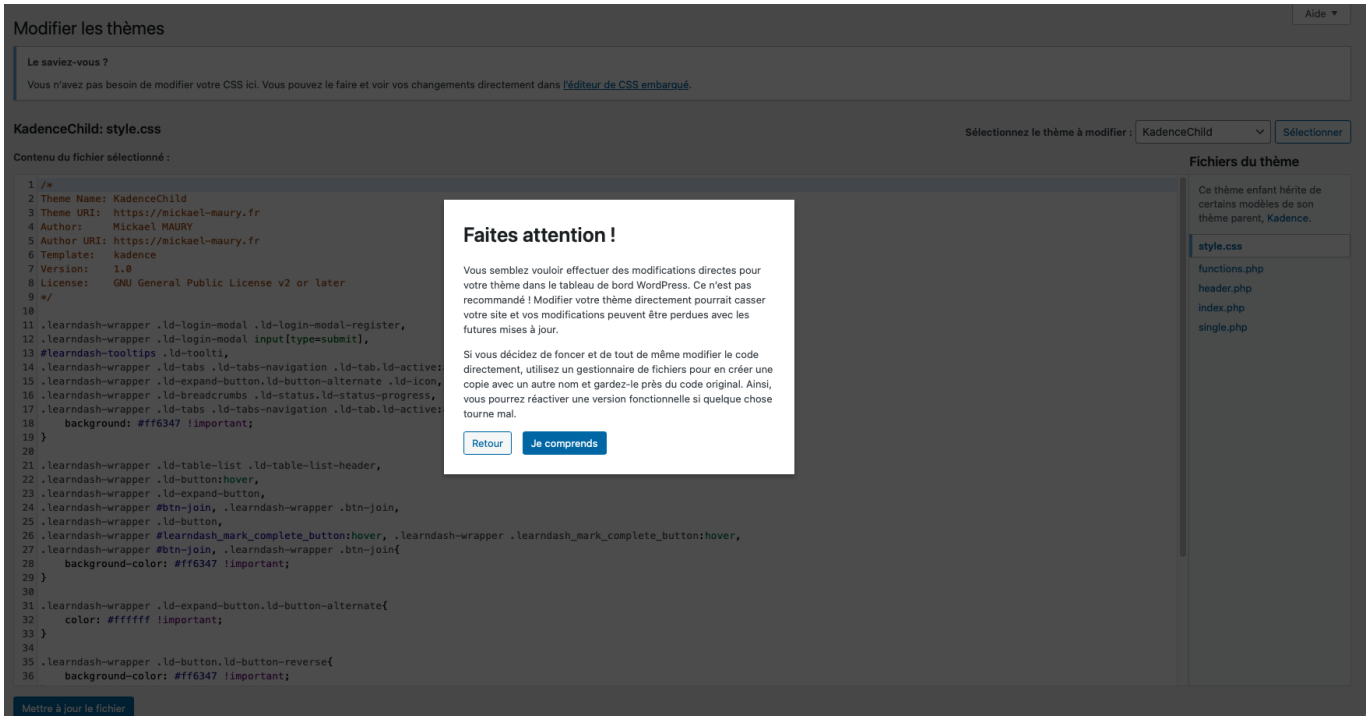
Comment WordPress gère l'authentification ?

WordPress utilise alors le **mot de passe saisi** auquel il ajoute la **clé de salage** afin de lancer le chiffrement et vérifier la correspondance en base de données avec le mot de passe stocké (chiffré).

Désactiver l'éditeur de fichiers

Ceci empêchera les utilisateurs administrateur d'avoir accès à l'édition du code des thèmes et plugins directement à partir du tableau de bord WordPress (**Apparence > Éditeur de fichiers des thèmes**).

Depuis la version WordPress 4.9, une alerte apparaît pour prévenir l'utilisateur qu'il s'agit d'une zone à risque.



Ceci représente un risque en termes de sécurité, tous les administrateurs n'ayant pas les compétences requises pour écrire du code.

De plus, si un hacker parvenait à s'infiltrer, il aurait accès à tous les fichiers en écriture.

Il est donc recommandé de désactiver cet éditeur.

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

Limiter le nombre de révisions

Pour limiter le nombre de révisions sur WordPress via le fichier **wp-config.php**, vous pouvez ajouter une constante dans ce fichier :

```
define('WP_POST_REVISIONS', 5);
```

Ce code limite le nombre de révisions à 5, vous pouvez modifier le nombre selon vos besoins.

Cela peut aider à réduire la taille de la base de données et à améliorer les performances de votre site WordPress.

Cette modification n'affecte que les futures révisions, les révisions existantes ne seront pas automatiquement supprimées.

Réduire l'intervalle d'enregistrement automatique

WordPress effectue des sauvegardes automatiques à intervalles réguliers, ce qui permet d'éviter la perte de contenu en cas de panne du navigateur ou de la connexion pendant que vous éditez un article ou une page.

Pour réduire l'intervalle d'enregistrement automatique sur WordPress via le fichier **wp-config.php**, vous pouvez ajouter une constante pour définir la fréquence à laquelle les sauvegardes automatiques sont effectuées.

```
define('AUTOSAVE_INTERVAL', 300); // En secondes
```

Ce code définit l’intervalle d’enregistrement automatique à 300 secondes (cinq minutes), vous pouvez modifier le nombre selon vos besoins.