CMS - WORDPRESS

Module 19 : Sécuriser son site

Objectifs

- Sécuriser son site

Sécuriser un site

- Faire des sauvegardes régulières, cela permet en cas de hack de pouvoir rétablir le site rapidement et de ne pas perdre tout le travail effectué sur le site web.
- Sans sauvegarde, vous risquez de repartir à zéro et de tout perdre.
- Personne n'est à l'abri d'une attaque, mais pour éviter de se faire hacker, suivez ces conseils :
  - Mettre à jour WordPress régulièrement pour sécuriser WordPress.
  - Mettre à jour les extensions et les thèmes qui corrige souvent des problèmes liés à la sécurité, ces problèmes étant rapportés par d'autres développeurs.
  - Utilisez des mots de passe complexes avec des majuscules, minuscules, chiffres et caractères spéciaux:
    - pour vos connexions au FTP,
    - aux bases de données,
    - au compte de votre hébergeur
    - et à l'administration.
  - Mettez des mots de passe différents pour chaque comptes.
  - Évitez d'enregistrer ces mots de passe sur votre ordinateur.

Sécuriser un site

- Évitez d'utiliser un nom simple lors de la connexion à l'administration du genre : admin.
- Utilisez une extension captcha pour les formulaires. Vous éviterez ainsi les spams.
  - Il en est de même pour les commentaires,
  - le formulaire de contact,
  - ou l'enregistrement sur le site.
- N'appelez pas votre base de données « WordPress »
  - c'est la première option qu'un hacker va tester pour se connecter à votre BD, puisque c'est le nom qui lui est donné par défaut.
  - Évitez d'installer phpMyAdmin sur le site de production ou alors sur une adresse différente.
- Masquez les erreurs de connexion à l'administration de WordPress.
  - Lors de la connexion à l'administration, WordPress indique si le mot de passe ou le nom est incorrect, une potentielle information à ne pas indiquer au hacker. Pour cela ajoutez ce **hook** au fichier **functions.php** :
    - add_filter('login_errors',create_function('$erreur', "return 'Erreur de connexion';"));

Sécuriser un site

- Changez les préfixes de tables. Lors de l'installation de votre site web, par défaut le préfixe de table est **wp_**.
- Il est alors facile pour un hacker de connaître la structure de votre base de données. Il faut donc changer les préfixes de tables. Si vous ne l'avez pas fait lors de l'installation, vous pouvez les modifier, grâce à des requêtes SQL.
- Dans un premier temps, changez le préfixe dans le fichier **wp-config.php** :
  - $table_prefix = 'wp_';
- Pour l'exemple, utilisez le préfixe : wp5_.
- Dans wp-config.php vous devez écrire :
  - $table_prefix = 'wp5_';

Sécuriser un site

- Puis, dans votre base de données, exécutez la requête SQL suivante, en changeant l'ancien préfixe par le nouveau grâce à la requête SQL RENAME :
  - Rename table ancienprefixe_commentmeta to nouveauprefixe_commentmeta;
  - Ce qui donne avec le préfixe wp5_ :
    - Rename table wp_commentmeta to wp5_commentmeta;
    - Rename table wp_comments to wp5_comments;
    - Rename table wp_links to wp5_links;
    - Rename table wp_options to wp5_options;
    - Rename table wp_postmeta to wp5_postmeta;
    - Rename table wp_posts to wp5_posts;
    - Rename table wp_termmeta to wp5_termmeta;
    - Rename table wp_terms to wp5_terms;
    - Rename table wp_term_relationships to wp5_term_relationships;
    - Rename table wp_term_taxonomy to wp5_term_taxonomy;
    - Rename table wp_usermeta to wp5_usermeta;
    - Rename table wp_users to wp5_users;

Sécuriser un site

- Si vous avez installé des extensions et qu'elles ont installé des tables, il faut également les renommer de la même manière.
- Il faut maintenant changer le préfixe dans la table d'options nouvellement renommée et la table **usermeta**, avec les requêtes SQL suivantes :
  - UPDATE `wp5_options` SET `option_name` = REPLACE(option_name, 'wp_', 'wp5_') WHERE `option_name` LIKE 'wp_%';
  - UPDATE `wp5_usermeta` SET `meta_key` = REPLACE(meta_key, 'wp_', 'wp5_') WHERE `meta_key` LIKE 'wp_%';
- Il faut également chercher à l'intérieur des tables des extensions l'ancien préfixe, afin de les renommer également.
- Utilisez des clés de sécurité. Ces clés de sécurité servent à crypter les cookies, elles se trouvent dans le fichier **wp-config.php**.
- Si elles ne sont pas présentes, vous pouvez en générer à l'adresse https://api.wordpress.org/secret-key/1.1/salt, et les remplacer dans le fichier **wp-config.php**.
- Exemple :
  - define('AUTH_KEY', '{G[#QqvW/QIM<qyw{gCYtK$_+f+%gc-8fT)~%6kbJ(5.NL=puMZp_jJ@J7T]7}B&');
  - define('SECURE_AUTH_KEY', 'Zˆ3YSKDb}o)wjD-x$}4-PEyz_E/a0h@*;W}w.<*/(<Z5to;8+@!_TS-SZr.eie}z');
  - define('LOGGED_IN_KEY', '~tˆcVs6sJ3 NJ5M+q3O5Tte%q54Qj(>4V7pV]wUTZhK;gf_M8zw|BS[+hyrrD9pd');
  - define('NONCE_KEY', ':hR!9p{/5M&`{Cr<1e_fQKtt;4i-$G[|ZxhC9Hs}DQUJ4nW+UT7KcY]j1/]DEABR');
  - define('AUTH_SALT', 'ELp{=w5I>|xK%AK3bOm:fatR96E`XL|(j*7Vuxw&V]+;#W];V*%P6g)5ED%%E|H');
  - define('SECURE_AUTH_SALT', '~f$njS.MyQ)EG,Q1JjeHPN!C-RK@C=3o7w-bWf|b|Oh=g$`zˆC?pP2ˆ&1Y*dzs[1');
  - define('LOGGED_IN_SALT', '%iG-p4/R8CZ~hQ?Ux8xk*HPToKCNFkoJtKC9@F_,0;wlWN[&=hrz[Bp4F0p2oF+K');
  - define('NONCE_SALT', ' Bm+38t,T~|606.4$CjzL-SST(I$[aK9%3,Ejb0~=K;.yXOAI|b454f8O~`biZL');

Sécuriser un site

- Pour éviter de lister les dossiers par défaut avec la configuration d'apache, utilisez un fichier index.php vide. Cela évite l'affichage de votre arborescence sur l'écran des internautes, qui verront ainsi une page blanche.
- Masquez la version de WordPress. Cela permet d'éviter à un hacker d'exploiter les failles connues liées à cette version de WordPress.
- La version de WordPress apparaît sur votre site web, soit dans le bas de page (auquel cas, supprimez cette ligne dans le fichier **footer.php**, soit dans les balises méta.
- Si dans le fichier **header.php** cette ligne apparaît, supprimez-la :
  - <meta name="generator" content="Wordpress <?php bloginfo ('version'); ?>" />
- Si la version apparaît toujours dans le code source de votre site, ajoutez cette action au fichier **functions.php** :
  - <?php remove_action('wp_head', 'wp_generator'); ?>
- Supprimez également le fichier **readme.html** à la racine du site WordPress, car il contient la version de WordPress.

Sécuriser un site

- Pour supprimer la version du site dans le **flux RSS** de WordPress, ajoutez au fichier **functions.php** ce code :
  - add_filter('get_the_generator_rss2', '__return_false');
  - add_filter('get_the_generator_atom', '__return_false');
- Empêchez l'accès de certains répertoires ou fichiers avec le fichier **.htaccess**.
- Protégez l'accès au fichier **wp-config.php** en ajoutant au fichier **.htaccess** le code suivant :
  - <FilesMatch ^wp-config.php$>
  - order allow,deny
  - deny from all
  - </FilesMatch>

Sécuriser un site

- Protégez l'accès au fichier **.htaccess** en lui ajoutant le code suivant :
  - <Files .htaccess>
  - order allow,deny
  - deny from all
  - </Files>
- Protégez l'accès aux dossiers en ajoutant au fichier **.htaccess** le code suivant :
  - Options All –Indexes
- Si vous faites des requêtes SQL dans vos thèmes ou extensions n'oubliez pas de sécuriser vos requêtes SQL, et vos champs de formulaires pour éviter toutes injections de code.

Sécuriser un site

- Utilisez la méthode **prepare()** de l'objet **wpdb** pour les requêtes SQL ou des fonctions PHP classiques, qui permettent de sécuriser l'insertion dans la base de données.
- En cas d'attaque de votre site, il faut au plus vite :
  - Nettoyer le site en supprimant les fichiers corrompus ou rétablir le site avec une sauvegarde (fichiers et base de données).
  - Changer le mot de passe de votre base de données
  - Remplacer le mot de passe dans le fichier **wp-config.php**
  - Changer le mot de passe de votre compte FTP.

Sécuriser un site

- Changer le mot de passe d'accès à l'interface d'administration de votre hébergeur.
- Changer le mot de passe de tous les administrateurs du site.
- Si vous avez plusieurs sites sur le même serveur:
  - il est préférable de vérifier l'intégralité des sites présents sur le serveur,
  - Un virus peut se propager et contaminer l'intégralité du serveur.
- Pour repérer les fichiers contaminés:
  - Télécharger les fichiers de votre site sur votre ordinateur en local
  - Vérifier que votre antivirus est activé et à jour.
  - Passer l'antivirus sur les fichiers téléchargés
  - Supprimer les fichiers détectés ou les mettre en quarantaine, puis les supprimer sur le serveur.
- Vous pouvez également utiliser des extensions comme Wordfence, Anti-Malware Security and Brute-Force Firewall, Cf. les plugins de Sécurité.