Sécuriser votre site sous Wordpress

La Cantine
20/03/2012

Marie Kuntz - Lézard Rouge

Sommaire

Avant de commencer

- Glossaire
  - **[bidouille]** : on rentre dans le code en essayant de ne pas tout casser
  - **[AV]** : fonction avancée, y aller prudemment
  - **attaque par force brute** : il s'agit de tester une par une toutes les combinaisons possibles (http://fr.wikipedia.org/wiki/Attaque_par_force_brute) ;
  - **injection sql** : consiste à passer des requêtes sql dans un formulaire pour forcer le passage
- Quelques conseils
  - Avant d'intervenir sur wordpress, faites toujours une sauvegarde

    1) de la base de données et

    2) du ou des fichiers que vous allez modifier

Principes généraux : wordpress

- Logiciel open-source
  - > tout le monde a accès au code source
  - > potentiellement, tout le monde peut trouver les failles de sécurité
- Outil de blog très utilisé
  - > il vaut mieux chercher des failles sur un logiciel très utilisé plutôt que sur un logiciel peu utilisé

Principes généraux : risques

- Défiguration du site
- Destruction des données et du site
- Vol de données (adresses emails des commentaires et collaborateurs, documents en accès restreint...)

Principes généraux : comment ?

- Attaque par force brute
- Injections SQL
- Exploitations des failles

Les bonnes pratiques
A l'installation

- Installer la dernière version
- Changer le login de base proposé (admin)
- mettre un mot de passe fort
- Tant qu'on y est : changer le préfixe des tables

Les bonnes pratiques
Note sur les mots de passe

- Deux paramètres :
  - Un mot de passe peut se composer de lettres majuscules, minuscules, chiffres et caractères spéciaux (lettres accentuées, ponctuation et autres @)
  - la longueur du mot de passe
- Nombre de combinaisons = nombre de possibilités (puissance) nombre de caractères.
  - un mot de passe de 6 caractères uniquement en minuscules = 26 puissance 6 soit 308 915 776 possibilités → hacké en 1 seconde par un PC bureautique...

Les bonnes pratiques
Après l'installation

- Par l'interface d'admin
  - Mettre à jour WP et les plugins
  - changer le login de base
  - mettre un mot de passe fort
  - changer le nom affiché des admins ; c'est ce nom qui apparaît quand vous laissez un commentaire ou que le nom du posteur est affiché dans les articles

Les bonnes pratiques
Après l'installation

- Le fichier wp-config.php
  - **[AV]** changer le préfixe des tables : aller dans phpMyAdmin et changer le préfixe des tables, puis aller dans wp-config.php, chercher la ligne $table_prefix = 'wp_'; et remplacer wp_ par le préfixe choisi.
  - **[bidouille]** clés de salage : les clés permettent d'améliorer l'authentification. Vous pouvez générer ces clés à cette adresse : https://api.wordpress.org/secret-key/1.1/salt/ cherchez les lignes define('AUTH_KEY',[...] et suivantes, remplacez par le texte généré par la page ci-dessus

Les bonnes pratiques
Après l'installation

- Le fichier functions.php (1/3)
  - supprimer le message d'erreur à la connexion

    Le risque : permet de savoir si le login est correct

    Ajouter le code suivant à la fin du fichier :

```
if ( ! function_exists("remove_login_error_messages")) {
  function remove_login_error_messages($val){
        $val = __('Same player plays again');
        return $val;
  }
}
add_filter('login_errors','remove_login_error_messages');
```

Les bonnes pratiques
Après l'installation

- Le fichier functions.php (2/3)
  - Suppression de la version de WP.

    Le risque : Permet de connaître la version de WP, et donc d'aller voir les failles correspondantes

    Ajouter le code suivant à la fin du fichier :

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

Les bonnes pratiques
Après l'installation

- Le fichier functions.php (3/3)
  - Suppression de la version des plugins

    Le risque : Permet de connaître la version des plugins, et donc d'aller voir les failles correspondantes

    Ajouter le code suivant à la fin du fichier :

```
if( !function_exists("delete_script_version")) {
   function delete_script_version( $src ){
       $parts = explode( '?', $src );
       return $parts[0];
   }
}
add_filter( 'script_loader_src', 'delete_script_version', 15, 1 );
add_filter( 'style_loader_src', 'delete_script_version', 15, 1 );
```

Les bonnes pratiques
Après l'installation

- [AV] Le fichier .htaccess (1/3)
  - Empêcher le listage des dossiers :

```
Options All -Indexes
```

Les bonnes pratiques
Après l'installation

- [AV] Le fichier .htaccess (2/3) :
  - Modifier le register_globals :

```
php_flag register_globals off
```

OU (OVH)

```
setEnv REGISTER_GLOBALS 0
```

Les bonnes pratiques
Après l'installation

- [AV] Le fichier .htaccess (3/3) :
  - Interdire l’accès aux fichiers importants

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

</files>

<files readme.html>
      order allow,deny
     deny from all

</files>

<files .htaccess>
     order allow,deny
     deny from all

</files>
```

Les bonnes pratiques
Les permissions de fichiers

- Note sur les permissions

Le système de permission sur les fichiers sous Linux

- des permissions pour le propriétaire du dossier/fichier
- des permissions pour le groupe
- des permissions pour les autres (ni propriétaire ni groupe)

3 types de permissions :

- Lire (r : read) => 4
- Ecrire (w : write) => 2
- Exécuter (x : execute) => 1

Les bonnes pratiques
Les permissions de fichiers

- Recommandé par WP :
  - / : racine du site (dossier www) : les fichiers devraient avoir une permission 640, sauf le fichier .htaccess s'il est généré par WP : indiquez alors 660.
  - /wp-admin/ : les dossiers doivent avoir une permission 750 et les fichiers 640
  - /wp-includes/ : les dossiers doivent avoir une permission 750 et les fichiers 640
  - /wp-content/ : 750 pour les dossiers et 640 pour les fichiers
    - Attention à /wp-content/plugins/ : les permissions peuvent varier selon les plugins

Les bonnes pratiques
Après l'installation – Mode parano

- accès à l'admin en SSL
  où : dans wp-config.php
  comment : ajouter la ligne suivante au début du fichier :
  `define('FORCE_SSL_ADMIN', true);`
  Note : il faut que votre hébergement accepte le https
- Autoriser votre seule adresse IP pour l'admin
  où : dans un .htaccess dans le répertoire wp-admin
  comment : mettre le code suivant :

```
AuthUserFile /dev/null
AuthGroupFile /dev/null
AuthName "Wordpress Admin Access Control"
AuthType Basic
order deny,allow
deny from all
allow from 123.456.789
```

  Note : nécessite une adresse IP fixe

Les bonnes pratiques
Après l'installation

- De l'utilisation des thèmes gratuits

  Peut contenir du code malicieux, du spam, des liens vers d'autres sites...

  http://www.wordpress-fr.net/2011/01/26/il-ne-faut-jamais-chercher-un-theme-wordpress-gratuit-sur-un-moteur-de-recherche/

Les bonnes pratiques
Après l'installation

- Les plugins
  - wp security scan : scanne et prévient les vulnérabilités (mots de passe, permissions sur les fichiers, …)
  - Login lockdown, login lock : permettent de bloquer la connexion après un certain nombre de tentatives,
  - AskApache Password protect : créé un .htaccess + .htpasswd pour avoir une pré-connexion à l'admin

Pour aller plus loin

- Sécuriser Wordpress
  http://codex.wordpress.org/Hardening_WordPress
- Les permissions de fichiers
  http://codex.wordpress.org/Hardening_WordPress#File_Permissions
  http://www.nightangel.fr/securiser-wordpress-securite-protection-pirates-
- Articles qui ont inspiré cette intervention
  http://www.creativejuiz.fr/blog/wordpress/wordpress-conseils-securite-bie
  http://www.hongkiat.com/blog/hardening-wordpress-security/
- Après avoir été hacké
  http://codex.wordpress.org/FAQ_My_site_was_hacked
- Mots de passe
  http://www.generateurdemotdepasse.com/
  http://howsecureismypassword.net/

Pour aller plus loin

- Plugins :

http://wordpress.org/extend/plugins/wp-security-scan/

http://wordpress.org/extend/plugins/login-lockdown/

http://wordpress.org/extend/plugins/askapache-password-protect/

http://www.lejournaldublog.com/securiser-votre-admin-wordpress/