Rendre votre installation de PrestaShop plus sûre

Rendre votre installation de PrestaShop plus sûre

Cette page liste plusieurs manières d'améliorer la sécurité de sa boutique PrestaShop.

N'importe qui peut les appliquer, quel que soit le niveau technique.

Utiliser toujours la dernière version de PrestaShop

Cela peut sembler être une évidence, mais on ne le répètera jamais assez. Les nouvelles versions de PrestaShop apportent de nouvelles fonctionnalités, des améliorations et des correctifs, et parmi ceux-ci peuvent se trouver des améliorations et correctifs liés à la sécurité.

L'équipe de PrestaShop travaille tous les jours à l'amélioration du logiciel, et s'efforce de proposer un outil sûr et sécurisé tant pour les marchands que pour leurs clients. Mais il peut y avoir des erreurs humaines, et les nouvelles versions sont là pour les corriger.

Il n'est pas toujours facile de mettre à jour PrestaShop, étant donné qu'une solution e-commerce est une somme complexe de fichiers, couplée au fait que vous devez mettre votre boutique en maintenant pendant quelques heures (ou parfois une journée entière, en fonction de la complexité de votre installation), ce qui signifie moins de visite de clients potentiels, et donc moins de ventes. Mais, dans le fond, vous préfèreriez certainement prendre le temps de vous assurer que votre boutiques et ses modules sont à jour, plutôt que de devoir gérer une attaque de hackers, ou des pertes de données privées.

Le module de mise à jour en 1 clic (disponible nativement) vous sera d'une grande aide, mais pensez toujours à bien faire des sauvegardes de vos fichiers et de votre base de données, dans le cas où un problème surviendrait.
Si le fait de faire une mise à jour automatique vous rend mal à l'aise, vous pouvez également suivre la méthode de mise à jour manuelle (mais elle prend bien plus de temps).
Dans les deux cas, faites d'abord des tests sur une copie de votre boutique, et assurez-vous que la copie a bien été mise à jour avant de mettre à jour votre site principal.

Mettez en place un mot de passe côté serveur pour le dossier de votre back-office

Vous pouvez établir une seconde protection par mot de passe afin de limiter encore plus l'accès à votre back-office (par exemple, `http://www.example.com/admin123456/`).

Pour mettre en place une authentification de base sur votre dossier d'administration, vous devez ajouter un fichier `.htaccess` et un fichier `.htpasswd` à ce dossier. Ce sont tous les deux de simples fichiers texte sans nom, seulement une extension.

Sous Windows, vous ne pouvez pas créer un fichier sans nom simplement. Il y a deux manières de résoudre ce problème :

- Vous pouvez nommer le fichier `htaccess.txt`, puis le mettre en ligne sur votre serveur FTP, et de là le renommer en `.htaccess`.
- Une astuce Windows consiste à nommer le fichier avec un point de chaque côté de son nom : "`.htaccess.`". Windows modifiera automatiquement le nom en "`.htaccess`".

L'un des buts du fichier `.htaccess` est de protéger vos dossiers et tous ceux qu'il contient (lire http://fr.wikipedia.org/wiki/.htaccess). **Cela ne fonctionne que pour les serveurs Apache**. Assurez-vous que vous utilisez un serveur Apache avant de créer un fichier `.htaccess`.

Pour protéger un dossier, vous devez mettre ces deux fichiers à la racine de ce dossier (par exemple, par le biais de votre logiciel FTP, dans le dossier `/var/www/prestashop/admin123456` ou peut-être `/public_html/prestashop/admin123456`).

Vous un exemple d'un fichier `.htaccess` :

```
AuthUserFile /var/www/.htpasswd
AuthName "Prestashop Admin Access"
AuthType Basic
Require valid-user
Options -Indexes
```

Explication :

- `AuthUserFile`: donne le lien du fichier contenant la liste des utilisateurs autorisés, et leurs mots de passe. `.htpasswd` est un fichier texte.
- `AuthName`: défini le message à afficher quand la fenêtre d'authentification s'affiche.
- `AuthType`: défini le type d'authentification.
- `Require`: demande à ce que les utilisateurs se connectent pour accéder au contenu. `valid-user` permet à plusieurs utilisateurs de se connecter et d'accéder au dossier.
- `Options`: défini les options du dossier. `-Indexes` désactive la génération automatique d'index de dossier, dans le cas où aucun fichier d'index n'est disponible.

Voici un modèle de contenu pour le fichier `.htpasswd` avec deux logins et leurs mots de passe :

```
login1:$apr1$/wJeliK8$e9OzgRaVL8J8wSsFBXjor1
login2:$apr1$yV65Kqqz$cFt3sV2.Q7hhLRRUJDo5a/
```

Ce fichier contient les identifiants et les "hash" des mots de passe de ceux qui sont autorisés à accéder au dossier (un hash est une "empreinte" unique d'une chaîne de caractère, permettant de l'identifier rapidement.
Vous pouvez générer les deux fichiers en passant par notre générateur en ligne : http://build.prestashop.com/tools/htaccess-generator-protect-your-prestashop-backoffice/
Pour créer le hash d'un mot de passe manuellement, vous pouvez passer par ce générateur de fichier `.htpasswd` : http://aspirine.org/htpasswd.html.

Il est chaudement recommandé de mettre ce fichier dans un dossier qui n'est pas accessible à vos applications web, donc au-dessus du dossier `/openbase_dir`. Cela empêche les injections au fichier `.htpasswd`, dans le cas où l'une de vos applications était vulnérable.

Il est également possible de limité l'accès par domaine ou adresse IP, via le fichier `.htaccess` :

```
Order Allow, Deny
Deny from all
Allow from .myprestashop.com
Allow from 127.0.0.1
```

Cependant, vous ne **devriez pas** utiliser cette sorte de directive :

```
<LIMIT GET POST>
Require valid-user
</LIMIT>
```

Utilisez des mots de passe plus sûrs

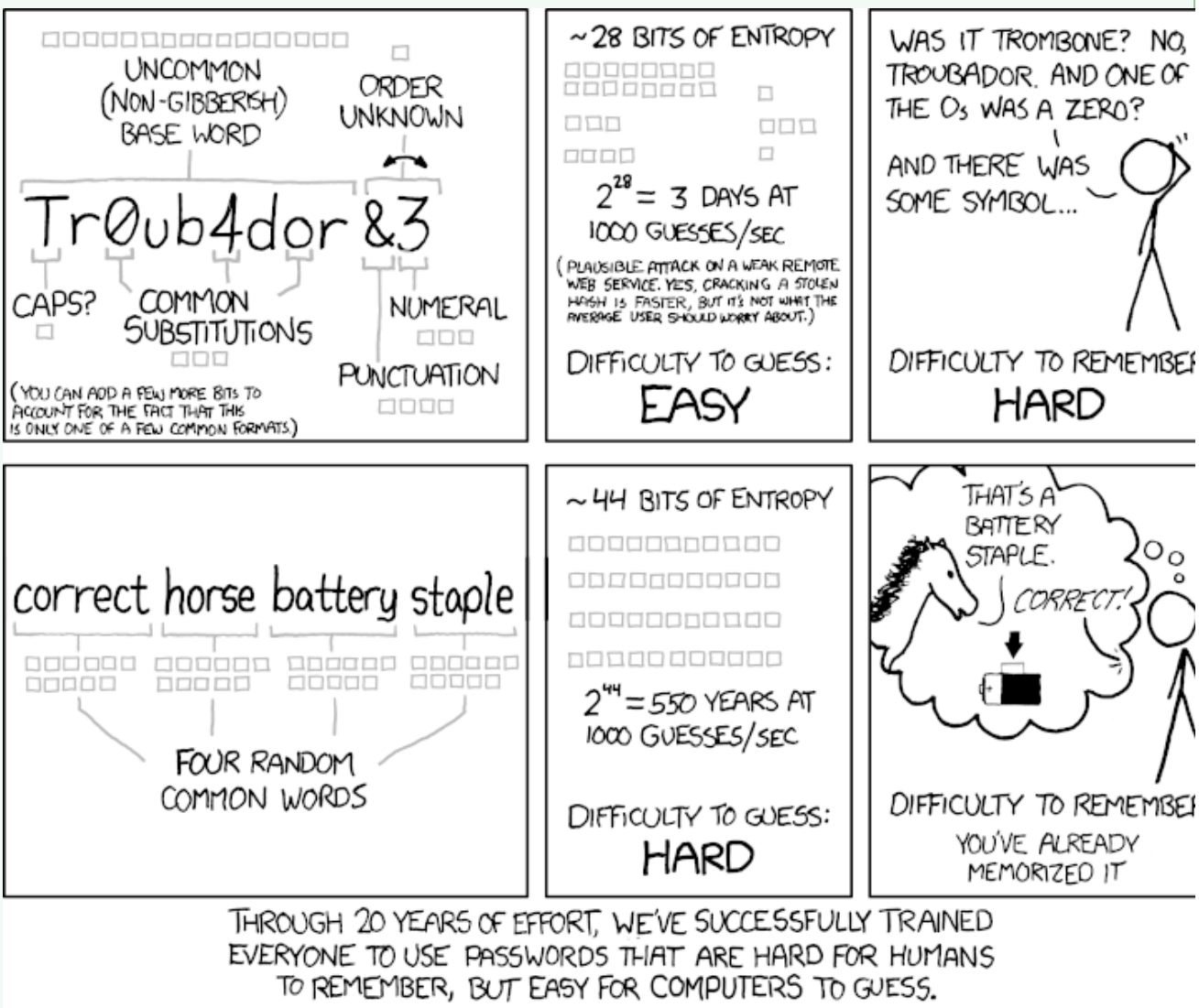
Choisissez un mot de passe complexe, fait d'un mélange de lettres, de chiffres et même de ponctuation, comme "5r3XaDR#". Vous pouvez, et devriez même, utiliser un générateur de mot de passe, comme celui de Symantec (http://www.pctools.com/guides/password/) ou celui de GRC (https://www.grc.com/passwords.htm).

Encore plus sûr qu'un mot de passe : vous pouvez utiliser un phrase de passe ("passphrase"). Une phrase de passe est non seulement plus simple à retenir, mais également plus difficile à hacker automatiquement (que ce soit par une attaque de force brute ou par dictionnaire).

Une phrase de passe n'a que besoin d'être longue et simple à mémoriser pour vous. N'importe quel dicton populaire peut faire l'affaire ("Ne pas jeter le bébé avec l'eau du bain"), mais une phrase absurde a encore moins de chance d'être découverte par un hacker. Par exemple, "Un grand envoie la tarte en orbite".

Il existe d'excellents générateurs de phrase de passe en ligne, qui vous aideront à trouver une phrase qui vous est unique. Par exemple : http://passphra.se/ ou http://www.fourmilab.ch/javascrypt/pass_phrase.html.

Le mots de passe de PrestaShop ne sont pas limités ni en nombre de caractères, ni en types de caractères.



(dessin original par by XKCD)

Changez le nom du dossier de votre back office

Renommez votre dossier /admin après l'installation de PrestaShop. C'est indispensable, et dans les faits vous ne pouvez pas accéder à votre back office avant d'avoir fait cette modification. Faites en sorte de choisir un nom réellement unique, idéalement un mélange de lettres et de chiffres, comme `/my4dm1n`, ou quoi que ce soit que vous puissiez facilement mémoriser.

Supprimez les fichiers par défaut inutiles

1. Supprimez toujours le dossier `/install` après avoir installé ou mis à jour PrestaShop.
2. Supprimez toujours ces fichiers inutiles de votre serveur de production :
    a. Le fichier README.md.
    b. Les fichiers CONTRIBUTING.md et CONTRIBUTORS.md.
    c. Le dossier `/docs` et l'ensemble de son contenu.

Bloquez l'accès à vos fichiers du thème

Vous pouvez interdire l'accès aux fichier/modèles de votre thème en ajoutant le contenu suivant à votre fichier `.htaccess` :

```
<FilesMatch "\.tpl$">
order deny,allow
deny from all
</FilesMatch>
```

Mettez à jour les logiciels de votre serveur

Le code de votre application PHP est le chemin le plus vulnérable de votre serveur. Il est donc fortement recommandé de régulièrement mettre à jour les applications de votre serveur : PHP, MySQL, Apache et toute autre application qui puisse se trouve sur votre hébergement web.