

Cours 15

Sécurité & Protection WP



Sécurité site WP

Les sites Wordpress souffrent de gros problèmes de sécurité car ils ont tous la même structure.

Exemple : wp-login.php la page de connexion est par défaut commune à tous les sites wordpress.

Les hackers utilisent les méthodes suivantes :

- **attaque de force brute (centaine à milliers d'attaques/jour)**
- **malwares (programme malveillant)**
- **spams**
- **robots**
- Etc

Exercices :

1. Changer de place
2. Tenter de se connecter au back-office du site de votre camarade
3. Tenter de naviguer entre les dossiers du site de votre camarade

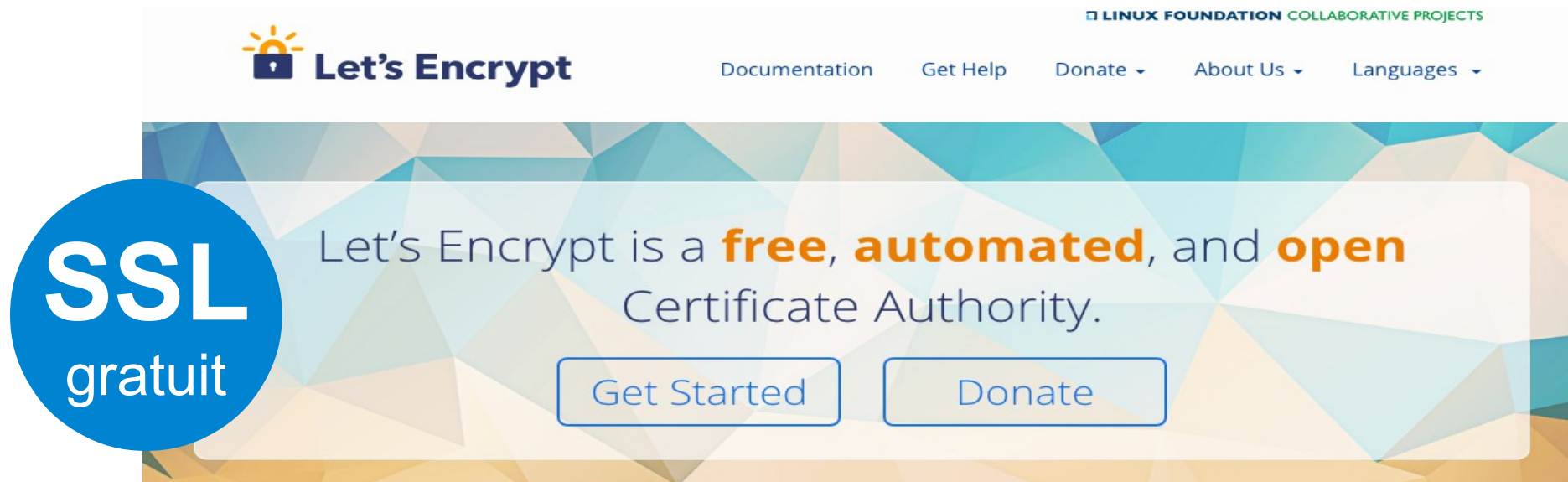
Certificat SSL (Secure Sockets Layer) dans l'hébergement web

Google recommande (impose) l'utilisation d'une adresse <https> pour assurer plus de sécurité.

La plupart des hébergeurs proposent désormais des hébergements web avec un certificat SSL, il est important de choisir un [hébergement web avec SSL](#).

Pour avoir une adresse sécurisée https, il faut :

- Activer le certificat SSL de son hébergement web (OVH, LWS, O2switch...)
- A défaut, obtenir un certificat gratuitement chez [Let's Encrypt](#) : <https://letsencrypt.org/>



Mesures de sécurité WP

1- Le compte Admin : Créez toujours un nouveau compte admin avec un login + mot de passe ultra sécurisé. Evitez un login avec votre prénom ou la racine de votre site.

2- Mot de passe : Il faut toujours utiliser des mots de passe complexes associant lettres, symboles et chiffres. Il vous faut employer de préférence un générateur de chaîne aléatoire de plus de 8 caractères.

3- Restreindre le nombre d'essais d'identification : Plusieurs plugins permettent de vous protéger des attaques par "force brute", c'est-à-dire les tentatives pour deviner votre mot de passe par une recherche de combinaisons possibles. Installez une extension de sécurité qui bloque les tentatives répétées d'une même adresse IP. (**Login Lock Down**, **iThemes**, **WordFence**, **Sucuri** par exemple). Si un robot tente d'entrer sur votre site, cela bloque l'accès pendant un certain temps. Une fois l'extension installée, vous pouvez paramétrer le nombre d'essais que vous voulez avant blocage et le temps de connexion après le blocage.

4- Masquer la version de votre WordPress, car elle donne des informations aux hackers pour trouver d'éventuelles failles de sécurité. Dans le fichier **functions.php** de votre thème, ajoutez ce bout de code :

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

Le numéro de version WP se trouve également dans le fichier **readme.html** situé à la racine de votre WordPress (fichier à supprimer également)

Mesures de sécurité WP

5- Faire des sauvegardes : Les backups du système sont à effectuer régulièrement pour prévenir un piratage ou un crash disque. **Duplicator, Back WP UP ou UpDraft+** sont des solutions pour la sauvegarde.

6- Soyez prudent lorsque vous téléchargez des templates (thèmes gratuits), ils peuvent révéler de nombreux virus. Pour vous protéger, installez un plugin comme : **Theme Authenticity Checker (TAC)**, celui-ci scanne et analyse les thèmes à la recherche d'un éventuel virus.

7- Faites des mises à jour régulières du site car cela permet d'avoir les dernières corrections des failles de sécurité. Encore une fois avant toute mise à jour, pensez à sauvegarder votre WP !

8- Ajouter les clefs de sécurité secrètes, les clés d'authentification SALT créent un cookie d'identification qui protège votre installation. Si ces codes ne sont pas présents dans votre fichier **wp-config.php**, vous pouvez les générer et les ajouter en vous rendant sur <https://api.wordpress.org/secret-key/1.1/salt/>

9- Protégez vos fichiers et bloquez la navigation dans vos dossiers WordPress. Par défaut, n'importe qui peut accéder au contenu de vos dossiers WordPress (**wp-content**) via un simple navigateur.

Mesures de sécurité WP

10- Changez le préfixe "wp_" par défaut des tables de la base MySQL (lors de la création). Ce préfixe est connu de tous et peut être vulnérable en cas d'injection.

11- Masquez les erreurs de connexion, WordPress renvoie un message bien trop explicite en cas de problème de connexion, ajouter la ligne suivante à votre `functions.php` du thème permet d'afficher un message d'erreur banalisé:

```
add_filter('login_errors',create_function('$a', "return null;"));
```

12- Déplacer votre PhpMyAdmin, cette application Web permet de gérer vos bases de données, située généralement à l'adresse suivante: /monsite.com/phpmyadmin, il est fortement recommandé de la déplacer (voir avec votre hébergeur).

13- Déplacer votre page de login, à l'aide d'un simple plugin tel que [WPS Hide Login](#) vous pouvez changer votre URL de connexion WordPress et limiter ainsi les attaques par "Brut Force" des hackers.

14- Choisissez un hébergement spécialisé WordPress. Avec un hébergeur WordPress, vous paierez plus cher les services de maintenance et sauvegarde, du coup votre site sera plus sécurisé. Ce type d'hébergement maintient, protège, répare et optimise votre site, incluant ainsi des services spécialisés pour Wordpress.

.htaccess : protection

Pour protéger le fichier wp-config via votre htaccess :

- 1- Ouvrir le fichier .htaccess dans Sublime Text ou Dreamweaver
- 2- **Pour protéger le fichier wp-config via votre htaccess**, ajoutez :

```
<Files wp-config.php>
```

```
    order allow,deny
```

```
    deny from all
```

```
</Files>
```

- 3- **Pour cacher les répertoires sensibles via le htaccess**, ajoutez :

```
Options All -Indexes
```

- 4- **Pour protéger le fichier htaccess lui-même**, ajoutez :

```
<Files .htaccess>
```

```
    order allow,deny
```

```
    deny from all
```

```
</Files>
```

Functions.php :

masquer les erreurs de login

1. Ouvrir le fichier functions.php du thème :
wp-content/themes/dyad/[functions.php](#)
2. Pour masquer les notifications d'erreurs trop explicites (informations à portée dangereuse pour les malwares), ajouter :

```
add_filter('login_errors',create_function('$a',  
"return null;"));
```


WPS Hide Login

WordPress.org Français

Accueil Thèmes **Extensions** Installation Téléchargement Versions Traduire WordPress Blog À propos

Extensions

Mes favoris Bêta test Développeurs

Rechercher des extensions



The banner features a large green padlock icon with a keyhole and three dots to its left. To the right is a blurred screenshot of a WordPress login form with fields for 'Identifiant' and 'Mot de passe', and buttons for 'Se souvenir de moi' and 'Se connecter'. The text 'WPS Hide Login' is centered at the bottom of the banner in a large, light gray font.

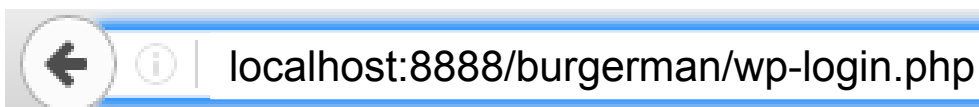
 **WPS Hide Login**
Par Remy Perona for WPSeurveur

Télécharger

WPS hide login

Le plugin WPS hide login : change l'url par défaut de connexion

[wp-login.php](#)



WORDPRESS

1. Installer le plugin
2. Aller dans les Réglages
3. Modifier l'[URL de connexion : admin-b4cx0f2iu9](#)
4. Sauvegarder la nouvelle adresse de connexion dans le fichier burgherman-infos-site.txt. Important !

WPS Hide Login
Besoin d'aide ? Essayez le [forum de support](#). Cette extension vous est gentiment proposée par [WPServeur](#).

URL de connexion

localhost:8888/burgherman/

admin-b4cx0f2iu9

Enregistrer les modifications

4. Enregistrer les modifications
5. Sauvegarder l'url de connexion et la tester

iThemes Security

WordPress.ORG Français

Accueil Thèmes Extensions Installation Téléchargement Versions Traduire WordPress Blog À propos

Extensions

Mes favoris Bêta test Développeurs

Rechercher des extensions

Better WP Security is now

iThemes Security

More than 30 ways to protect your site from attacks.

 iThemes Security (anciennement Better WP Security)

Par iThemes

Télécharger

iThemes Security

Ithemes Security est un puissant plugin pour assurer la sécurité totale et la sauvegarde de votre site avec les fonctionnalités de :

- 1- Security Check** : scan intégral du site pour détecter les problèmes, erreurs, dysfonctionnements et failles de sécurité du site
- 2- Réglages principaux** : pour contrôler les options de sécurité
- 3- Mode Absent** : rendre indisponible le back-office durant une période
- 4- Utilisateurs bannis** : faire une liste d'utilisateurs bannis (liste d'IP bannis)
- 5- Local Brute Force Protection** : protection contre les attaques de force brute
- 6- Détection 404** : bloque automatiquement les IP cherchant les pages 404 (not found : pages inexistantes) à exploiter
- 7- Sauvegarde de la Base de Données** : et stockage en local ou envoi par mail
- 8- Détection de changement de fichiers** : détecte une modification de fichier
- 9- File permissions** : Diagnostic et recommandations des droits et permissions d'accès aux fichiers (changer les droits d'accès via le logiciel FTP)
- 10- Network Brute Force Protection** : réseau de site de reporting et protection
- 11- SSL** : assure une connexion sécurisée entre le serveur et l'internaute (https)
- 12- Modifications systèmes et Wordpress** : modifications avancées de sécurité
- 13- Salages** : met à jour une clé secrète pour augmenter la sécurité de wordpress
- 14- etc.

iThemes Security

- 1- Installer l'extension
- 2- Activer l'extension
- 3- Aller dans les Réglages :
pour configurer l'extension

7.3. iThemes – Security Check

×

Security Check


- ✓ Your site is now using Network Brute Force Protection.
- ✓ Changed the REST API setting in WordPress Tweaks to "Restricted Access".
- ✓ Utilisateurs bannis is enabled as recommended.
- ✓ Sauvegarde de la base de données is enabled as recommended.
- ✓ Local Brute Force Protection is enabled as recommended.
- ✓ Strong Password Enforcement is enabled as recommended.
- ✓ Modifications WordPress is enabled as recommended.



Run Secure Site Again

Close

iThemes – Tableau de bord

Parcourir et cliquer sur les fonctionnalités pour les configurer

 New! The iThemes Security dashboard just got a new look. [See what's new](#) ×

All (30) | Recommended (24) | Advanced (6)

Security Check

Ensure that your site is using the recommended features and settings.

[Configure Settings](#)

Réglages principaux

Configure basic settings that control how iThemes Security functions.

[Configure Settings](#)

Détection 404

Automatically block users snooping around for pages to exploit.

[Learn More](#) [Enable](#)

Mode Absent

Disable access to the WordPress Dashboard on a schedule.

[Learn More](#) [Enable](#)

Utilisateurs bannis

Block specific IP addresses and user agents from accessing the site.

[Configure Settings](#) [Disable](#)

Local Brute Force Protection

Protect your site against attackers that try to randomly guess login details to your site.

[Configure Settings](#) [Disable](#)

Sauvegarde de la base de données

Create backups of your site's database. The backups can be created manually and on a schedule.

Détection de changement de fichiers

Monitor the site for unexpected file changes.

[Learn More](#) [Enable](#)

File Permissions

Lists file and directory permissions of key areas of the site.

[Configure Settings](#)


Obtenir iThemes Security Pro

Add an extra layer of protection to your WordPress site with [iThemes Security Pro](#), including:

- Two-factor authentication
- Scheduled malware scanning
- Google reCAPTCHA integration
- Private, ticketed support
- + more Pro-only features

[Obtenir iThemes Security Pro](#)

Télécharger notre guide de poche sur la Sécurité WordPress



iThemes – Réglages principaux

×

Réglages principaux

The following settings modify the behavior of many of the features offered by iThemes Security.

Écrire sur les fichiers	<input checked="" type="checkbox"/> Allow iThemes Security to write to wp-config.php and .htaccess. <i>Whether or not iThemes Security should be allowed to write to wp-config.php and .htaccess automatically. If disabled you will need to manually place configuration options in those files.</i>
E-mail de notification	<div>toutanck.picalive@gmail.com</div> <i>Adresse(s) e-mail(s) à laquelle toutes les notifications de sécurités seront envoyées. Une adresse par ligne.</i>
Envoyer un e-mail de résumé	<input type="checkbox"/> Envoyer un e-mail de résumé <i>Durant les périodes de forte attaque ou à d'autres moments, une extension de sécurité peut générer BEAUCOUP d'e-mails juste pour vous dire qu'elle fait son travail. Activer cette option permettra de</i>

Save Settings

iThemes – Utilisateurs bannis

×

Utilisateurs bannis

Cette fonction vous permet de bannir complètement les hôtes et les agents utilisateurs de votre site sans avoir à gérer une configuration particulière de votre serveur. Toutes les adresses IP ou les agents utilisateurs présents dans les listes ci-dessous ne seront pas autorisés à accéder à votre site.

Liste noire par défaut

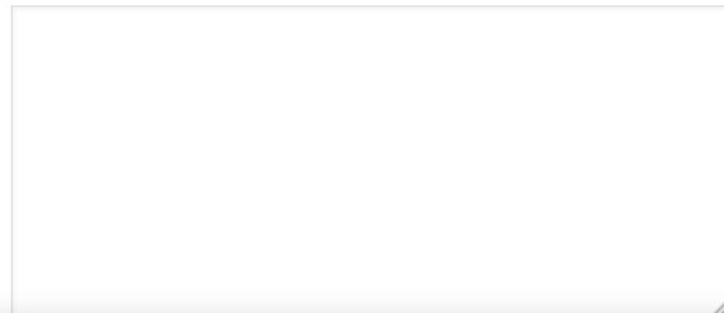
☐ Activer la fonctionnalité de liste noire de HackRepair.com

As a getting-started point you can include the blacklist developed by Jim Walker.

Ban Lists

☒ Enable Ban Lists

Hôtes bannis



Save Settings

Disable

iThemes – Local Brute Force Protection

x

Local Brute Force Protection

If one had unlimited time and wanted to try an unlimited number of password combinations to get into your site they eventually would, right? This method of attack, known as a brute force attack, is something that WordPress is acutely susceptible to as, by default, the system doesn't care how many attempts a user makes to login. It will always let you try again. Enabling login limits will ban the host user from attempting to login again after the specified bad login threshold has been reached.

À propos des blocages

Your lockout settings can be configured in [Global Settings](#).

Vos réglages actuels sont configurés comme suit :

- **Permanently ban:** oui
- **Number of lockouts before permanent ban:** 3
- **How long lockouts will be remembered for ban:** 7
- **Host lockout message:** Erreur
- **User lockout message:** Vous avez été bloqué suite à un trop grand nombre de tentatives de connexion erronées.
- **Is this computer white-listed:** oui

Maximum de tentatives de
connexions atteintes par
hôte

Tentatives

Nombre de tentatives qu'un utilisateur peut faire avant que son hôte ou son ordinateur ne soit bloqué. Mettre à 0 pour enregistrer le nombre de

Save Settings

Disable

iThemes – Sauvegarde de la Base de Données

×

Sauvegarde de la base de données

Une des meilleures façons de vous protéger d'une attaque est d'avoir accès à une copie de la sauvegarde de la base de données de votre site. Si quelque chose se passe mal, vous pourrez restaurer votre site en restaurant la base de donnée à partir d'une sauvegarde et remplacer les fichiers en même temps. Utilisez le bouton ci-dessous pour créer une sauvegarde de votre base de données qui servira à cela. Vous pouvez également planifier des sauvegardes automatiques et télécharger ou supprimer les sauvegardes précédentes.

Press the button below to create a database backup using the saved settings.

Create a Database Backup

Sauvegarder l'ensemble de la base de données

☒ **Cochez cette case vous permettra de sauvegarder l'ensemble des tables de votre base de données, même si elles ne font pas parties de votre site WordPress.**

Méthode de sauvegarde

Enregistrer localement et envoyer par e-mail

Méthode de sauvegarde enregistrée
Choisissez ce que nous devrions faire avec votre fichier de sauvegarde. Vous pouvez l'envoyer par e-mail, l'enregistrer localement ou les deux.

Emplacement de la

/home/toutanck/www/cmaformation/wpps/cma/wp-content/uploads/

Save Settings

Disable

iThemes – Salages Wordpress

x

Salages WordPress

A secret key makes your site harder to hack and access by adding random elements to the password.

In simple terms, a secret key is a password with elements that make it harder to generate enough options to break through your security barriers. A password like "password" or "test" is simple and easily broken. A random, unpredictable password such as "88a7da62429ba6ad3cb3c76a09641fc" takes years to come up with the right combination. A salt is used to further enhance the security of the generated result.

Note that changing the salts will log you out of your WordPress site.

**Changer les salages
WordPress**

☐

Check this box and then save settings to change your WordPress Salts.

Save Settings

iThemes – Modifications Wordpress

×

Modifications WordPress

Ce sont des réglages avancés qui peuvent être utilisés pour renforcer la sécurité de votre site WordPress.

Note : Ces réglages sont répertoriés comme avancée, car ils bloquent les formes courantes d'attaques, mais ils peuvent aussi bloquer les plugins et thèmes légitimes qui s'appuient sur les mêmes techniques. En activant les réglages ci-dessous, nous vous recommandons de faire un par un pour vérifier que tout sur votre site fonctionne toujours comme prévu.

Rappelez-vous que certains de ces réglages peuvent entrer en conflit avec d'autres plugins ou thèmes. Il faut donc tester votre site après l'activation de chacun de ces réglages.

En-tête Windows Live Writer

☐ Remove the Windows Live Writer header.

Ce n'est pas nécessaire si vous n'utilisez pas Windows Live Writer ou d'autres clients de blogs qui utilisent ce fichier.

Modifier l'URI d'en-tête

☐ Remove the RSD (Really Simple Discovery) header.

Retirer l'en-tête RSD (Really Simple Discovery). Si vous n'avez pas intégré votre blog avec un système externe XML-RPC comme Flickr, alors la fonction RSD est pratiquement inutile.

Commentaire indésirable

☐ Réduire le spam sur les commentaires

Cette option empêchera les robots sans référent ni user-agent identifiés

Save Settings

Disable

iThemes – Détection de changement de fichier

×

Détection de changement de fichiers

Even the best security solutions can fail. How do you know if someone gets into your site? You will know because they will change something. File Change detection will tell you what files have changed in your WordPress installation alerting you to changes not made by yourself. Unlike other solutions, this plugin will look only at your installation and compare files to the last check instead of comparing them with a remote installation thereby taking into account whether or not you modify the files yourself.

Enable

Wordfence Security



Inscription Se connecter

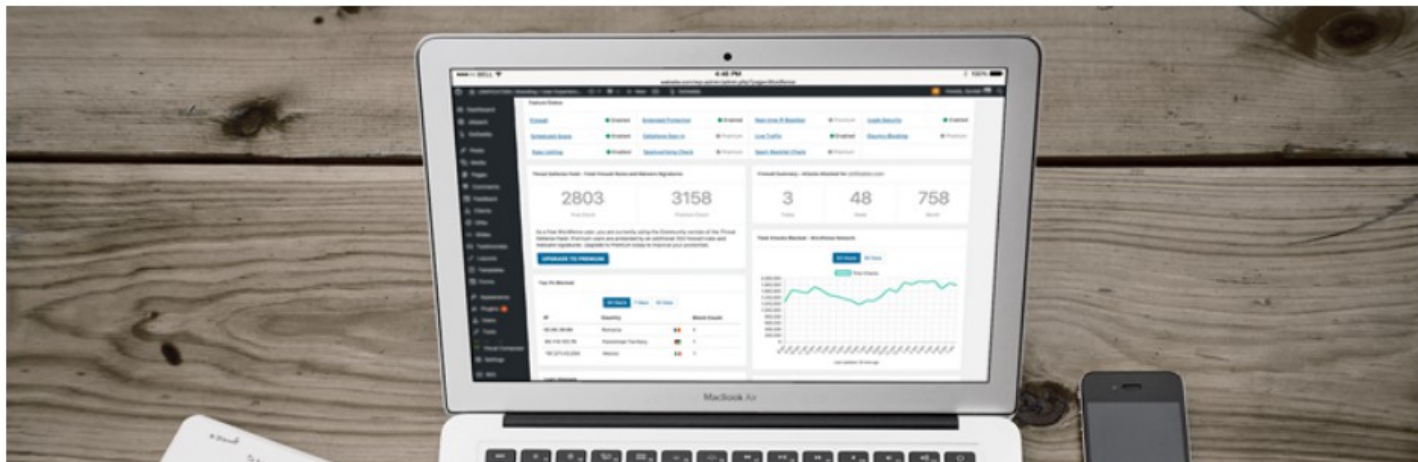
 **WORDPRESS.ORG** Français

[Accueil](#) [Thèmes](#) [Extensions](#) [Installation](#) [Téléchargement](#) [Versions](#) [Traduire WordPress](#) [Blog](#) [À propos](#)

Extensions

[Mes favoris](#) [Bêta test](#) [Développeurs](#)

Rechercher des extensions



Wordfence Security

Par Wordfence

Télécharger

Wordfence Security

Wordfence Security assure la sécurité du site WP avec ses fonctionnalités de :

- 1- Dashboard** : tableau de bord récapitulatif de la sécurité
- 2- Scan et diagnostic du site WP** : révélant les problèmes, dysfonctionnements, erreurs et failles de sécurité...
- 3- Firewall** : pare-feu pour sécuriser le site avec blacklist (IP non-autorisé) et whitelist (IP autorisé)...
- 4- Blocking** : pour bloquer les IP des malwares, IP de pays...
- 5- Live traffic** : statistiques de trafic du site
- 6- Tools** : outils d'audit, connexion via 06, Whois (IP)...
- 7- Options** : passer en premium (payant) pour plus de fonctionnalités de sécurité

Wordfence - Dashboard

Last scan completed: 19 July 2017 19 h 21 min

No security problems detected

Notifications

No notifications received

Feature Status

Firewall	● Enabled	Extended Protection	● Disabled	Real-time IP Blacklist	● Premium	Login Security	● Enabled
Scheduled Scans	● Enabled	Cellphone Sign-in	● Premium	Live Traffic	● Enabled	Country Blocking	● Premium
Rate Limiting	● Enabled	Spamvertising Check	● Premium	Spam Blacklist Check	● Premium		

Threat Defense Feed - Total Firewall Rules and Malware Signatures

4073	4584
Free Count	Premium Count

As a free Wordfence user, you are currently using the Community version of the Threat Defense Feed. Premium users are protected by an additional 511 firewall rules and malware signatures. Upgrade to Premium today to improve your protection.

UPGRADE TO PREMIUM

Firewall Summary - Attacks Blocked for [www.toutanck-pubalive.fr/cmaformation/wpps/cma](#)

0	0	0
Today	Week	Month

Total Attacks Blocked - Wordfence Network

24 Hours

30 Days

Wordfence - Scan

Scan

Scheduling

Options

[Learn more about scanning](#)

START A WORDFENCE SCAN

[Click to kill the current scan.](#)

Scan Summary

[Jul 19 19:21:32] Preparing a new scan.

[Jul 19 19:21:32] Scanning for old themes, plugins and core files

[Jul 19 19:21:32] Scan complete. You have 3 new issues to fix. See below.

Done.
Problems found.
Scan Complete.

You are running the Wordfence Community Scan signatures.

The Wordfence Scan alerts you if you've been hacked

As new threats emerge, the Threat Defense Feed is updated to detect these new hacks. The Premium version of the Threat Defense Feed is updated in real-time protecting you immediately. As a free user **you are receiving the community version** of the feed which is updated 30 days later.

GET PREMIUM

Scan Detailed Activity


[Jul 19 19:21:32] Initiating quick scan

[Jul 19 19:21:32] -----

[Jul 19 19:21:32] Quick Scan Complete. Scanned in less than 1 second.

[Email activity log](#)

Upgrade Your Protection




Wordfence Premium customers receive firewall rules, malware signatures and malicious IP updates in real time.

GET PREMIUM

Have you been hacked?

Our team of security experts will clean the infection and remove malicious content. Once your site is restored we will provide a detailed report of our findings.

All for an affordable rate.



Wordfence - Firewall

Web Application Firewall

Brute Force Protection

Rate Limiting

[Learn more about the Wordfence Web Application Firewall](#)

The Wordfence Firewall stops you from getting hacked

As new threats emerge, the Threat Defense Feed is updated to protect you from new attacks. The Premium version of the Threat Defense Feed is updated in real-time protecting you immediately. As a free user **you are receiving the community version** of the feed which is updated 30 days later.

GET PREMIUM

Protection Level ⓘ

Basic WordPress Protection

Optimize the Wordfence Firewall

Firewall Status ⓘ


Learning Mode

☒ Automatically switch to Enabled Mode on 07/26/2017 07:21pm +0:

When you first install the Wordfence Web Application Firewall, it will be in learning mode. This allows Wordfence to learn about your site so that we can understand how to protect it and how to allow normal visitors through the firewall. We recommend you let Wordfence learn for a week before you enable the firewall.

SAVE

Upgrade Your Protection




Wordfence Premium customers receive firewall rules, malware signatures and malicious IP updates in real time.

GET PREMIUM

Have you been hacked?

Our team of security experts will clean the infection and remove malicious content. Once your site is restored we will provide a detailed report of our findings.

All for an affordable rate.



Security Expert

Wordfence - Blocking

Wordfence Live Activity: Wordfence used 512 KB of memory for scan. Server peak memory usage was: 42.75 MB

Blocked IPs | Country Blocking | Advanced Blocking

[Learn more about Blocked IPs](#)


[Clear all blocked IP addresses](#) | [Clear all locked out IP addresses](#)

You can manually (and permanently) block an IP by entering the address here:

IPs blocked from accessing the site | **IPs locked out from login** | IPs throttled for accessing the site too frequently

No IP addresses have been blocked yet. If you manually block an IP address or if Wordfence automatically blocks one, it will appear here.


Upgrade Your Protection



Wordfence Premium customers receive firewall rules, malware signatures and malicious IP updates in real time.

Have you been hacked?

Our team of security experts will clean the infection and remove malicious content. Once your site is restored we will provide a detailed report of our findings.



Wordfence – Live Traffic

Wordfence Live Activity: Wordfence used 512 KB of memory for scan. Server peak memory usage was: 42.75 MB

Human

Bot

Warning


Blocked

Filter Traffic:

All Hits

Show Advanced Filters

Upgrade Your Protection



Wordfence Premium customers receive firewall rules, malware signatures and malicious IP updates in real time.

GET PREMIUM

Wordfence - Tools

Password Audit

Whois Lookup

Cellphone Sign-in

Diagnostics

[Learn more about Password Auditing](#)

Password Auditing is only available to Premium Members

Wordfence Password Auditing uses our high performance password auditing cluster to test the strength of your admin and user passwords. We securely simulate a high-performance password cracking attack on your password database and will alert you to weak passwords. We then provide a way to change weak passwords or alert members that they need to improve their password strength.

Upgrade today:

- Receive real-time Firewall and Scan engine rule updates for protection as threats emerge
- Other advanced features like IP reputation monitoring, an advanced comment spam filter, advanced scanning options, cell phone sign-in and country blocking give you the best protection available
- Access to Premium Support
- Discounts of up to 90% available for multiyear and multi-license purchases

GET PREMIUM

Start a Password Audit

Audit your site passwords by having us securely simulate a password cracking attempt using our high performance servers. Your report will appear here and you can easily alert your users to a weak password or change their passwords and email them the change.

Select the kind of audit you would like to do


Audit administrator level accounts (extensive audit against a large dictionary of approx. 260 Million)

Notify when ready

Results will appear on this page. We will email you when they're ready.

Start Password Audit

Upgrade Your Protection




Wordfence Premium customers receive firewall rules, malware signatures and malicious IP updates in real time.

GET PREMIUM

Have you been hacked?

Our team of security experts will clean the infection and remove malicious content. Once your site is restored we will provide a detailed report of our findings.

All for an affordable rate.



Wordfence - Options

[Learn more about Wordfence Options](#)

License

Your Wordfence API Key [i](#)

26edec4b25dd7de359929c8a80b91e04a1061c2b98c1dcdb38be69d0bdd6416a13f671b7c357fe

Key type currently active

The currently active API Key is a **Free Key**. [Click Here to Upgrade to Wordfence Premium now.](#)

Upgrade today:

- Receive real-time Firewall and Scan engine rule updates for protection as threats emerge
- Advanced features like IP reputation monitoring, country blocking, an advanced comment spam filter and cell phone sign-in give you the best protection available
- Remote, frequent and scheduled scans
- Access to Premium Support
- Discounts of up to 90% for multiyear and multi-license purchases

GET PREMIUM

Basic Options [i](#)

Enable Rate Limiting and Advanced Blocking [i](#)



NOTE: This checkbox enables ALL blocking/throttling functions including IP, country and advanced blocking, and the "Rate Limiting Rules" below.

Enable login security [i](#)



Upgrade Your Protection



Wordfence Premium customers receive firewall rules, malware signatures and malicious IP updates in real time.

GET PREMIUM

Have you been hacked?

Our team of security experts will clean the infection and remove malicious content.



Etat de santé (à partir de WP 5.2)

Outils > Santé du site

La fonctionnalité d'état de santé du site permet d'obtenir un bilan de santé du site avec la détection des problèmes et des recommandations d'amélioration.

Santé du site 65%

StatutInfo

État de santé du site

La vérification de santé du site affiche des informations critiques à propos de votre configuration WordPress et les éléments qui nécessitent votre attention.

2 problèmes critiques

Title tag	Search Engine Optimization
Description meta tag	Search Engine Optimization


4 améliorations recommandées

Vous devriez retirer les thèmes inactifs	Sécurité
Nous vous recommandons de mettre à jour PHP	Performance
Serveur SQL obsolète	Performance

Etat de santé

Outils > Santé du site

Il permet d'obtenir un bilan de santé général de son site grâce à un panel de points de contrôle lancés de façon automatique et des informations de débogage qui sont précieuses pour votre hébergeur ou pour les responsables techniques de votre site.

Santé du site 

État

Informations

Information de santé du site

Cette page peut vous afficher chaque détail à propos de la configuration de votre WordPress. Si nous voyons ici quoi que ce soit qui puisse être amélioré, nous vous le ferons savoir sur la page de l'état de santé.

Si vous souhaitez exporter une liste de toutes les informations contenues dans cette page, vous pouvez utiliser le bouton ci-dessous pour les copier dans votre presse-papier. Vous pourrez ensuite les coller dans un fichier texte pour les enregistrer sur votre ordinateur, dans un e-mail d'échange avec un support technique, ou encore avec une développeuse ou un développeur de thème/extension.

Copier les informations du site dans le presse-papier

WordPress



Répertoires et tailles



Thème actif



Autres thèmes (10)



Extensions indispensables (2)



Extensions actives (25)



Prise en charge des médias



Mode de récupération

Fatal Recovery Mode

WordPress intègre maintenant nativement un « mode de récupération » (recovery mode en anglais).

Protection contre les erreurs fatales PHP

L'idée est simple : si un thème ou une extension plante votre site, plutôt que de vous fournir un classique « écran blanc de la mort » à partir duquel vous ne pouvez plus rien faire, WordPress désactivera automatiquement le thème ou l'extension associé au bug. Si cela se passe en votre absence (via une mise à jour automatique par exemple) alors vous recevrez un e-mail contenant des informations sur le bug rencontré et sur le fait que votre site est passé en mode de récupération.

Vie et sécurité du site WP

La vie et la sécurité du site Wordpress démarrent lorsque le site est en ligne et accessible à tous.

Il est important d'être vigilant et mettre en place des mesures de sécurité, protection et sauvegarde régulières. Lorsque les outils sont en place, il faut les analyser et ajuster.

Il faut mettre à jour les versions de Wordpress et mettre à jour régulièrement les plugins, thèmes et le contenu du site pour qu'il vive.

Avant chaque mise-à-jour de plugin ou thème, par sécurité, il faut faire une sauvegarde avec Duplicator par exemple (car il y a toujours un risque d'erreur...).

White Screen Of Death

WSOD : Ecran blanc

Il y a un certain nombre de causes pour l'écran blanc de la mort et il est donc difficile de cerner la source du problème. Cependant, les points suivants sont considérés comme étant les causes les plus communes :

- Plugin incompatible avec la version actuelle de WordPress
- Conflit avec un autre plugin
- Incompatibilité avec le thème actif et un plugin

Thème incompatible avec la dernière version de WordPress (principalement quand un nouveau thème est installé ou un ancien est mis à jour)

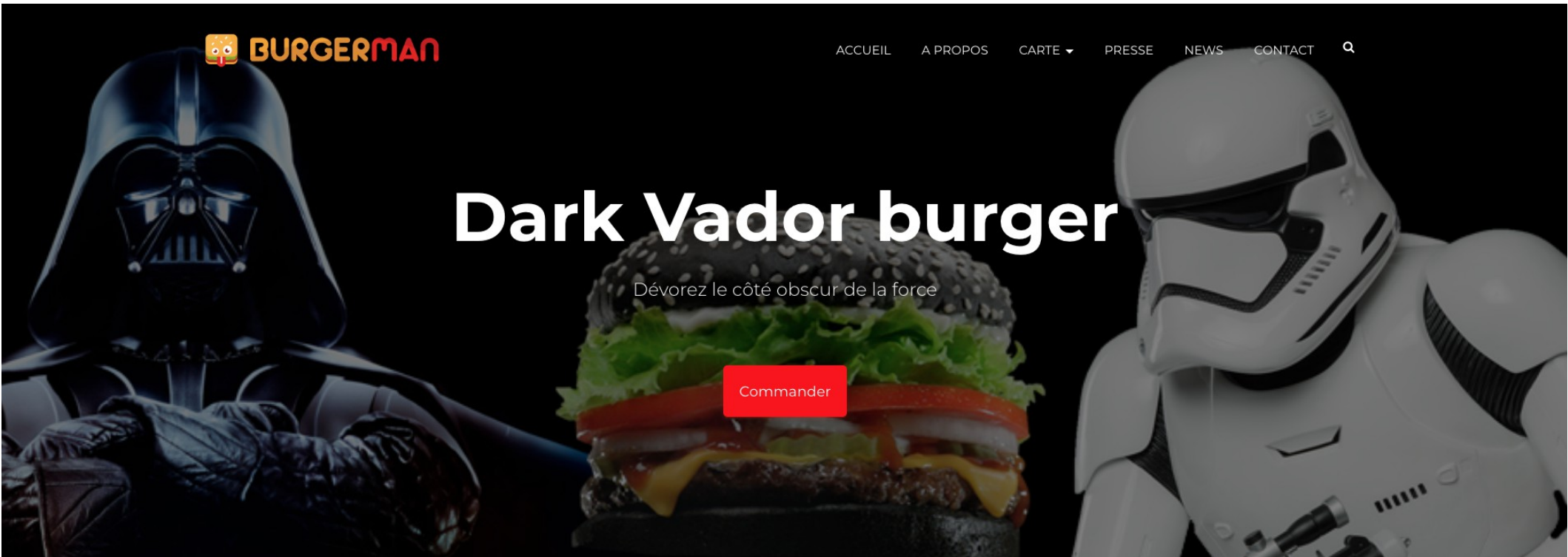
La plupart des hébergeurs propose la restauration du serveur à 1 jour, 3 jours, 3 semaines, 1 mois... Ainsi si votre site plante à cause d'un événement, vous pouvez le restaurer à une date où tout fonctionnait...

Ressources / solutions en cas de problèmes d'installation :

<https://wpformation.com/solutions-erreurs-wordpress/>

<https://www.wpexplorer.com/fixes-wordpress-white-screen/>

BurgerMan site : FIN



Ressources web + Wordpress



Ressources Wordpress

- <https://fr.wordpress.org/>
- <https://wpmarmite.com/>
- <https://wpformation.com/wordpress/>
- <https://wpchannel.com/>
- <http://www.geekpress.fr/>
- <https://www.gregoirenoyelle.com/>
- Etc

N'oubliez-pas : quels que soient la fonctionnalité, le problème sur Wordpress, la solution existe !

Thèmes Wordpress

- <https://fr.wordpress.org/themes/>
- <https://www.elegantthemes.com/>
- <https://www.elegantthemes.com/gallery/divi/>
- <https://colorlib.com/wp/free-bootstrap-wordpress-themes/>
- <https://themeforest.net/>
- <http://pinegrow.com/docs/wordpress/>
- <https://market.envato.com/>
- Etc

Plugins Wordpress

- **Référencement :**

<https://fr.wordpress.org/plugins/wordpress-seo/>

<https://fr.wordpress.org/plugins/all-in-one-seo-pack/>

<https://fr.wordpress.org/plugins/google-analytics-for-wordpress/>

- **Formulaire :**

<https://fr.wordpress.org/plugins/jetpack/>

<http://www.gravityforms.com/>

- **Multilingue :**

<https://wpml.org/fr/>

- **E-commerce, Widgets, sliders :**

<https://woocommerce.com/>

<https://woocommerce.com/woosidebars/>

Sauvegarde & Sécurité Wordpress

Quelques articles et solutions pour la sécurité de votre site WP :

- <https://wpformation.com/11-rappels-securite-wordpress/>
- <https://www.notuxedo.com/piratage-wordpress/>
- <https://wpmarmite.com/brute-force-wordpress/>
- <https://vigilance.fr>

Plugins de sécurité, sauvegarde etc :

- <https://fr.wordpress.org/plugins/wps-hide-login/>
- <https://fr.wordpress.org/plugins/wordfence/>
- <https://fr.wordpress.org/plugins/better-wp-security/>
- <https://fr.wordpress.org/plugins/backwpup/>
- <https://codecanyon.net/item/hide-my-wp-amazing-security-plugin-for-wordpress/4177158>
- <https://fr.wordpress.org/plugins/sucuri-scanner/>
- <https://fr.wordpress.org/plugins/jetpack/>

Ressources Web

- Typographie :

<http://www.dafont.com/fr/>

<https://www.fontsquirrel.com/>

- Couleurs :

<https://color.adobe.com/fr/>

<http://www.colorzilla.com/gradient-editor/>

- Icônes :

<https://design.google.com/icons/>

- Courbes de bézier :

<http://bezier.method.ac/>

- Développement :

<http://www.w3schools.com/>

<https://openclassrooms.com/>

Bilan de formation

Logiciels et Technologies utilisés

- Wordpress
- Mamp
- Photoshop
- Dreamweaver ou
- Sublime Text

