



SÉCURISER WORDPRESS

Lausanne WordPress Meetup
21/12/2017

SUPERHUIT

CONTENU

Sécurité ?
Installation
Setup avancé
Compte utilisateur
Mises à jour
Plugins

FELIPE PAUL MARTINS



aka. *Kuuak*

Frontend developer chez Superhuit

Dans l'informatique depuis 2004
WordPress depuis 2015

Superhuit

Agence digitale Porto-Lausannoise
fondée en 2013

<https://www.linkedin.com/in/felipe-paul-martins/>

<https://profiles.wordpress.org/kuuak>

<https://github.com/kuuak>

superhuit.ch

SUPERHUIT

1. SÉCURITÉ

Pourquoi sécuriser mon blog/site ?

SÉCURITÉ

Insertion de liens (SEO spam)

Vol de données

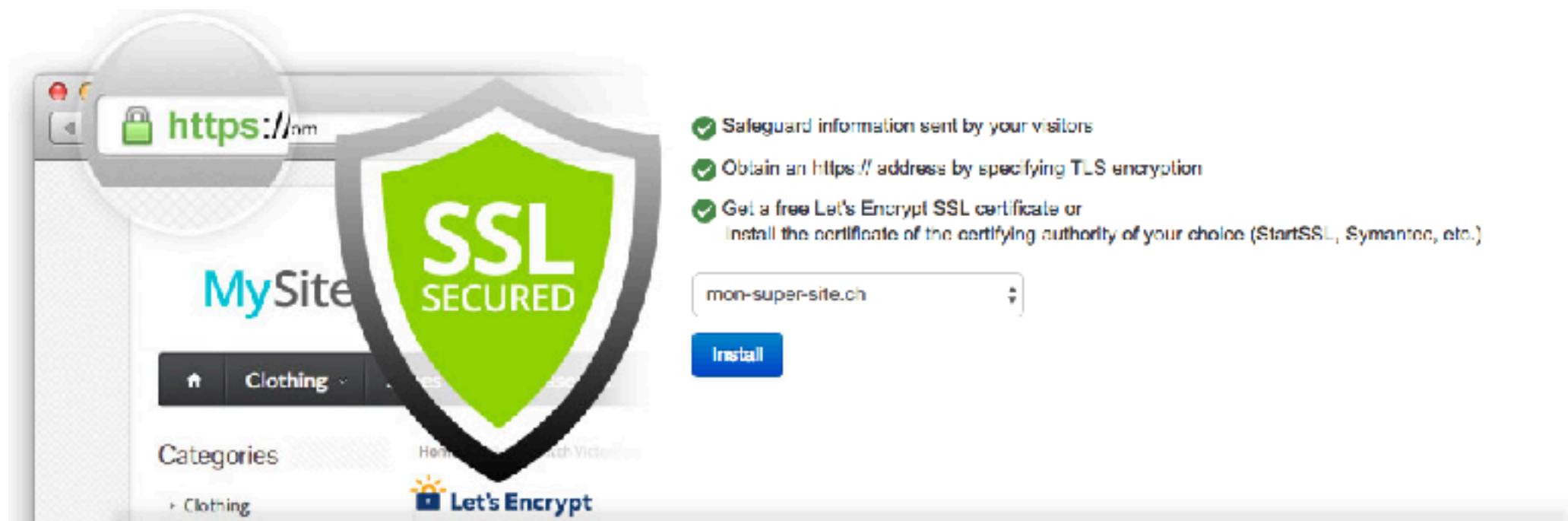
Gain financier (par ex. Ransomware)

Injection de programmes malicieux

2. INSTALLATION

Comment sécuriser WordPress lors de l'installation

2.0 ACTIVER HTTPS



Certificat SSL

Let's Encrypt gratuit

GUI chez les Hébergeurs

2.1 INSTALLATION

Télécharger WordPress depuis le site officiel
wordpress.org



The image shows the WordPress database connection setup screen. It features the classic blue 'W' logo at the top. Below it, a message reads: "Vous devez saisir ci-dessous les détails de connexion à votre base de données. Si vous ne les connaissez pas, contactez votre hébergeur." The form contains five input fields with their respective descriptions:

Nom de la base de données	<input type="text" value="db_my_super_site"/>	Le nom de la base de données avec laquelle vous souhaitez utiliser WordPress.
Identifiant	<input type="text" value="user_db-site"/>	Nom d'utilisateur MySQL.
Mot de passe	<input type="text" value="pqajPqaNaZ2vwKukBcezT"/>	Votre mot de passe de base de données.
Adresse de la base de données	<input type="text" value="localhost"/>	Si localhost ne fonctionne pas, demandez cette information à l'hébergeur de votre site.
Préfixe des tables	<input type="text" value="mss_"/>	Si vous souhaitez faire tourner plusieurs installations de WordPress sur une même base de données, modifiez ce réglage.

A "Valider" button is located at the bottom left of the form.

2.2 BASE DE DONNÉES

Si possible éviter les valeurs par défaut

Changer le prefix des tables



Bienvenue

Bienvenue dans la très célèbre installation en 5 minutes de WordPress ! Vous n'avez qu'à remplir les informations demandées ci-dessous et vous serez prêt à utiliser la plus extensible et puissante plateforme de publication de contenu au monde.

Informations nécessaires

Veuillez renseigner les informations suivantes. Ne vous inquiétez pas, vous pourrez les modifier plus tard.

Titre du site

Identifiant
Les identifiants ne peuvent utiliser que des caractères alphanumériques, des espaces, des tirets bas ("_"), des traits d'union ("-"), des points et le symbole @.

Mot de passe  Cacher
Forte

Important : Vous aurez besoin de ce mot de passe pour vous connecter. Pensez à le stocker dans un lieu sûr.

Votre adresse de messagerie
Vérifiez bien cette adresse de messagerie avant de continuer.

Visibilité pour les moteurs de recherche Demander aux moteurs de recherche de ne pas indexer ce site
Certains moteurs de recherche peuvent décider de l'indexer malgré tout.

[Installer WordPress](#)

2.3 COMPTE ADMINISTRATEUR

Eviter l'identifiant **admin** !

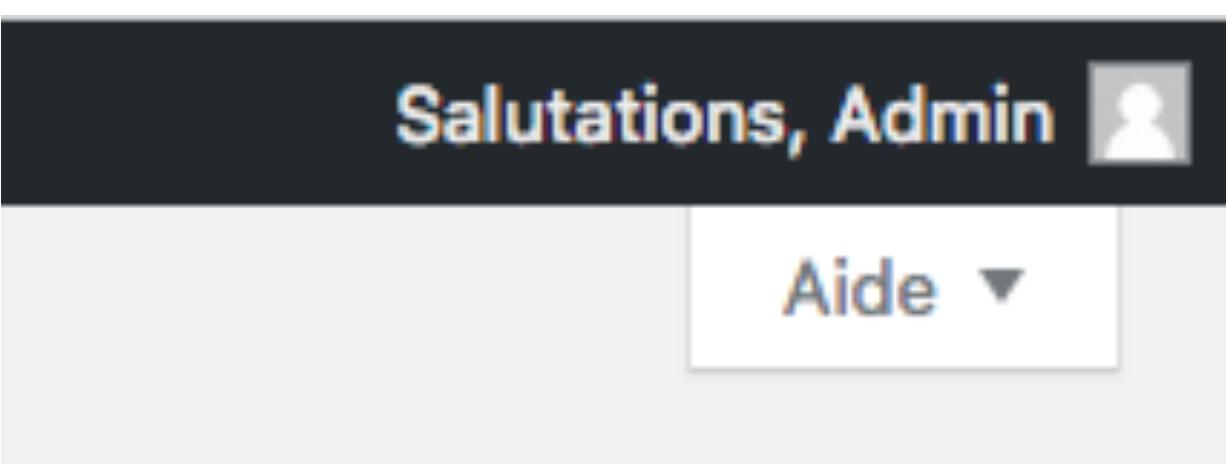
Mot de passe unique et difficile

Screenshot of a user profile edit form. The sidebar shows 'Utilisateurs' is selected. The main form fields are:

Nom	
Identifiant	Adm1n15Trat0r
Prénom	
Nom	
Pseudonyme (nécessaire)	Admin
Nom à afficher publiquement	Admin
Informations de contact	
Adresse de messagerie (nécessaire)	me@localhost.local

2.3 COMPTE ADMINISTRATEUR

Ne pas afficher
publiquement l'identifiant



MOTS DE PASSE

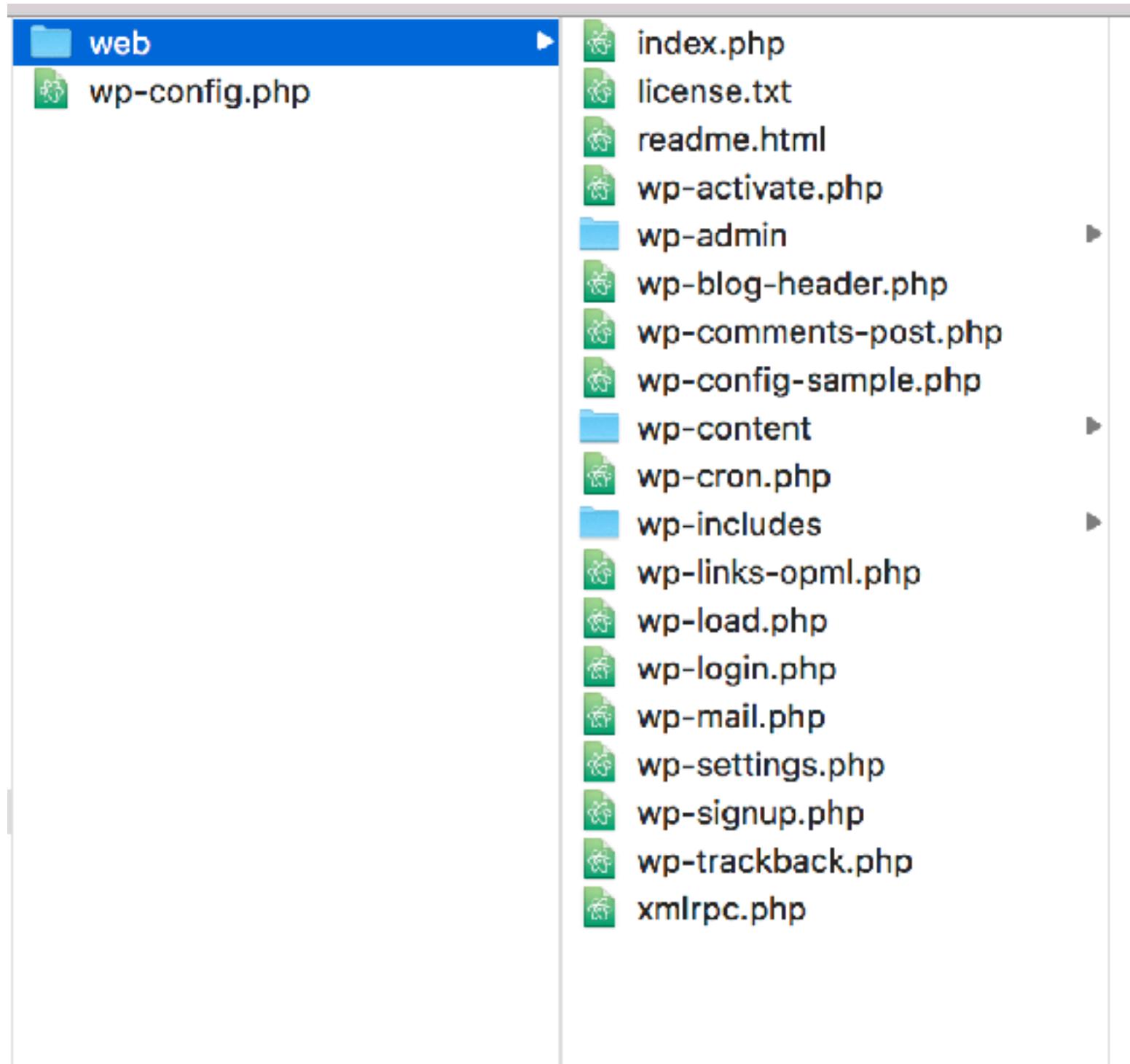
Unique pour chaque site/service

Un grand nombre de caractères

Gestionnaire de mots de passe

3. SETUP AVANCÉ

Quelques manipulations avancées pour améliorer la sécurité



3.1 DÉPLACER LE FICHIER WP-CONFIG.PHP

Il est possible de déplacer le fichier **wp-config.php** dans le répertoire parent.

3.2 PERMISSIONS DES FICHIERS

Vérifier et changer la permission des fichiers et dossiers

Fichiers: 755

Dossiers: 644

wp-config.php: 600

```
find /path/to/your/wordpress/install/ -type d -exec chmod 755 {} \;
find /path/to/your/wordpress/install/ -type f -exec chmod 644 {} \;
chmod 600 /path/to/your/wordpress/install/wp-config.php
```

Médias

Pages

Commentaires

Apparence

Thèmes

Personnaliser

Widgets

Menus

En-tête

Éditeur

Extensions 1

Utilisateurs

Outils

Réglages

Réduire le menu

Modifier les thèmes

Twenty Seventeen: Feuille de style (style.css)

Sélectionnez le thème à modifier : Twenty Seventeen Séle

```
/*
Theme Name: Twenty Seventeen
Theme URI: https://wordpress.org/themes/twentyseventeen/
Author: the WordPress team
Author URI: https://wordpress.org/
Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a focus on business sites, it features multiple sections on the front page as well as widgets, navigation and social menus, a logo, and more. Personalize its asymmetrical grid with a custom color scheme and showcase your multimedia content with post formats. Our default theme for 2017 works great in many languages, for any abilities, and on any device.
Version: 1.3
License: GNU General Public License v2 or later
License URI: http://www.gnu.org/licenses/gpl-2.0.html
Text Domain: twentyseventeen
Tags: one-column, two-columns, right-sidebar, flexible-header, accessibility-ready, custom-colors, custom-header, custom-menu, custom-logo, editor-style, featured-images, footer-widgets, post-formats, rtl-language-support, sticky-post, theme-options, threaded-comments, translation-ready

This theme, like WordPress, is licensed under the GPL.
Use it to make something cool, have fun, and share what you've learned with others.
*/
----->>> TABLE OF CONTENTS:
-----
```

[Mettre à jour le fichier](#)

Modèles

- Modèle pour l'erreur (404.php)
- Archives (archive.php)
- Commentaires (comments.php)
- Pied de page du thème (footer.php)
- Page d'accueil statique (front-page.php)
- Fonctions du thème (functions.php)
- En-tête du thème (header.php)
- back-compat.php (inc/back-compat.php)
- color-patterns.php (inc/color-patterns.php)
- custom-header.php (inc/custom-header.php)
- customizer.php (inc/customizer.php)
- icon-functions.php (inc/icon-functions.php)
- template-functions.php

3.3 DÉSACTIVER L'ÉDITEUR DE FICHIER

Ajouter dans le fichier wp-config.php

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

The screenshot shows a WordPress login screen. At the top is the classic blue 'W' logo. Below it, a red error message box contains the text "ERREUR : Nom d'utilisateur non valide. [Mot de passe oublié ?](#)". Below the message are two input fields: "Nom d'utilisateur ou adresse e-mail" and "Mot de passe". To the left of the "Nom d'utilisateur" field is a checkbox labeled "Se souvenir de moi". To the right of the "Mot de passe" field is a blue "Se connecter" button.

This screenshot shows a similar WordPress login screen. The error message at the top reads "ERREUR : ce mot de passe ne correspond pas à l'identifiant Adm1n15TratOr. [Mot de passe oublié ?](#)". The "Nom d'utilisateur ou adresse e-mail" field contains the text "Adm1n15TratOr". The "Mot de passe" field is empty. The "Se souvenir de moi" and "Se connecter" buttons are present.

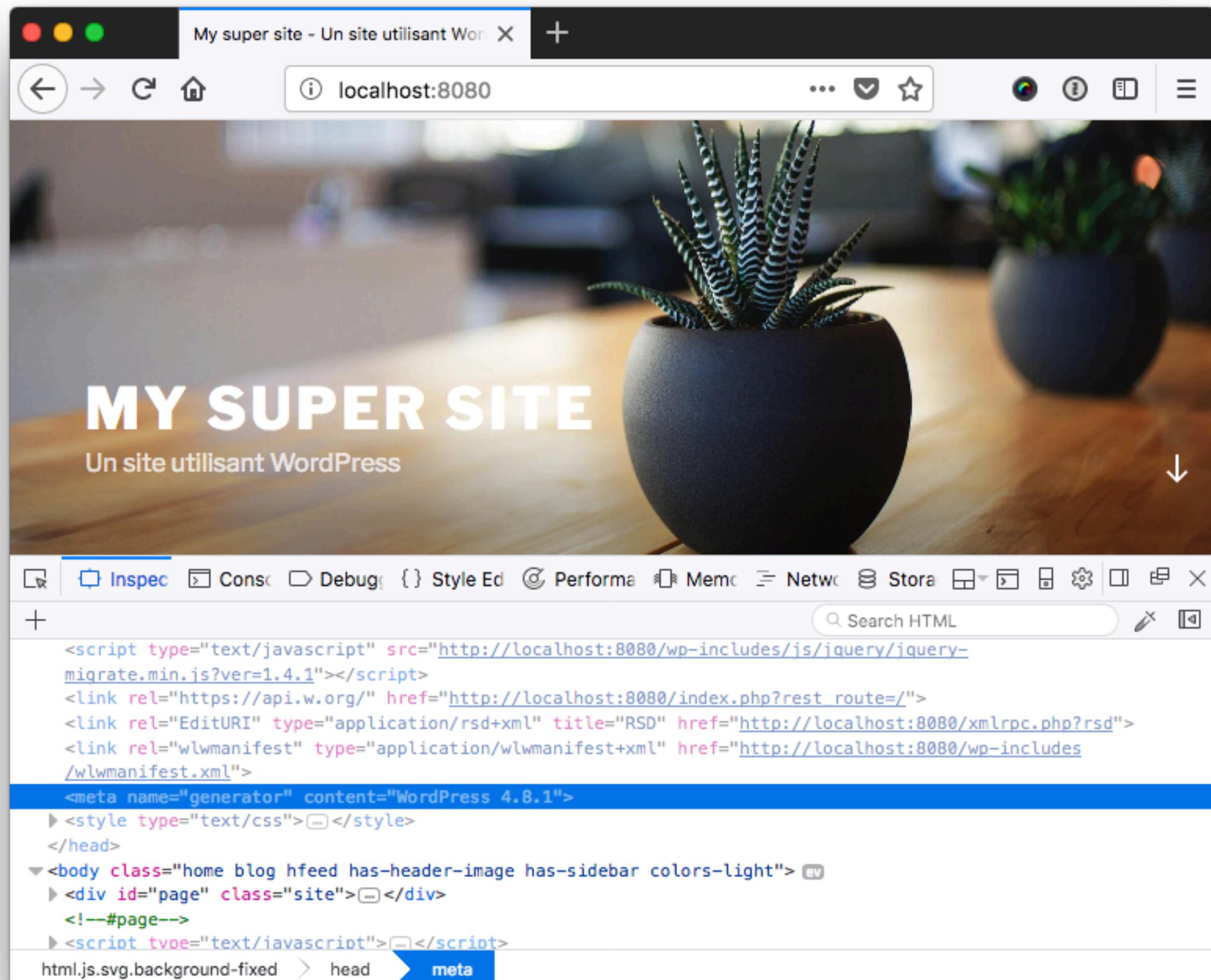
3.4 MASQUER LES ERREURS DE LOGIN

Ne pas donner d'information supplémentaire aux hacker

The screenshot shows a WordPress login screen with a red error message box containing the text "Mauvais identifiants". The "Nom d'utilisateur ou adresse e-mail" field contains "admin" and the "Mot de passe" field is empty. The "Se souvenir de moi" and "Se connecter" buttons are visible.

Ajouter au fichier functions.php

```
add_filter('login_errors',  
create_function('$no_login_error',  
"return 'Mauvais identifiants';"));
```



3.6 MASQUER LA VERSION DE WORDPRESS

Supprimez la balise
“generator”
Ajouter dans functions.php

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

Désactiver les erreurs PHP*

Ajouter en haut du fichier
wp-config.php

```
error_reporting(0);  
@ini_set('display_errors', 0);
```

*certains hébergeurs ne l'autorisent pas

3.5 AUTRES MESURES

Bloquer l'exécution de scripts php
dans les répertoires
/wp-content/uploads/
/wp-includes/

Ajouter un fichier .htaccess

```
<Files *.php>  
deny from all  
</Files>
```

4. COMPTES UTILISATEURS

A-t-on vraiment besoin de 18 administrateurs?

Role	Posts
Administrator	3
Administrator	0
Administrator	0
Administrator	0
Administrator	2
Administrator	29
Role	Posts
6 items	

4.1 ADMINISTRATEUR



User Role Editor

Select Role and change its capabilities: Éditeur (editor)

Show capabilities in human readable form Show deprecated capabilities

Group (Total/Granted) Quick filter: Granted Only

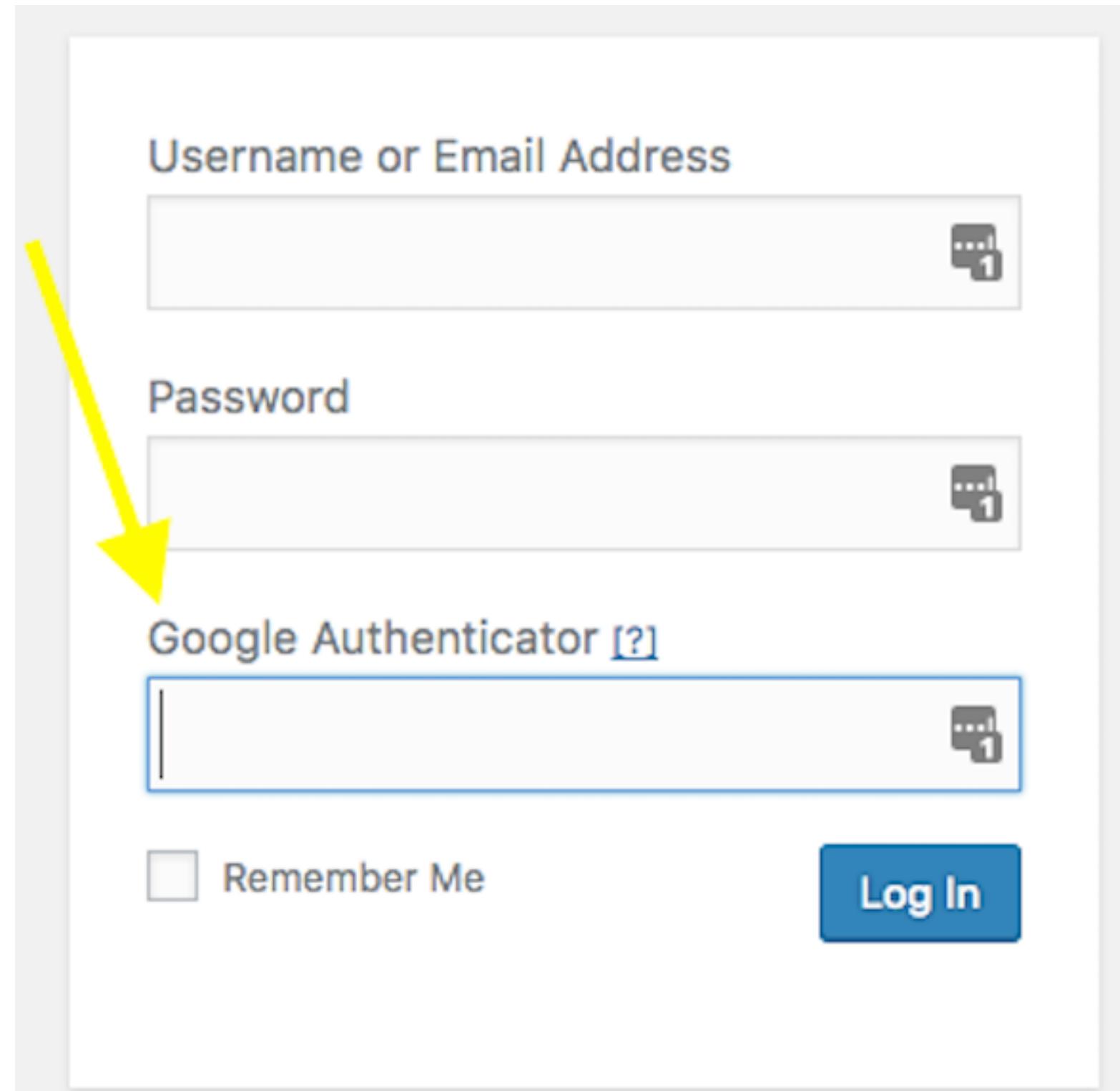
Group	Total	Granted
All (72/35)	72	35
- Core (61/34)	61	34
- General (12/6)	12	6
- Themes (6/0)	6	0
- Posts (12/12)	12	12
- Pages (10/10)	10	10
- Plugins (5/0)	5	0
- Users (6/0)	6	0
- Deprecated (12/8)	12	8
- Custom Post Types (11/10)	11	10
- Groupes de champs (11/10)	11	10
- Champs (11/10)	11	10
- Custom capabilities (10/1)	10	1
- User Role Editor (7/0)	7	0
- Yoast SEO (3/1)	3	1

activate_plugins
 create_posts
 create_users
 delete_others_pages
 delete_others_posts
 delete_pages
 delete_plugins
 delete_posts
 delete_private_pages
 delete_private_posts
 delete_published_pages
 delete_published_posts
 delete_themes
 delete_users
 edit_dashboard
 edit_others_pages
 edit_others_posts
 edit_pages
 edit_plugins
 edit_posts
 edit_private_pages
 edit_private_posts
 edit_published_pages
 edit_published_posts
 edit_theme_options
 edit_themes
 edit_users
 export
 import
 install_plugins
 install_themes
 list_users
 manage_categories
 manage_links
 manage_options
 moderate_comments

4.2 PLUS DE RÔLES

Plus de granularité

Plugin: User Role Editor



4.3 AUTHENTIFICATION DEUX FACTEURS

Deux étapes au lieu d'une

Besoin d'un accès physique à un « device »

Plugins:

Auto: <https://wordpress.org/plugins/authy-two-factor-authentication/>

Duo: <https://wordpress.org/plugins/duo-wordpress/>

Google Authenticator: <https://wordpress.org/plugins/google-authenticator/>

5. MISES À JOUR

Never more safe than updated

5.1 NUMERO DE VERSION

Semantic Versioning

Majeur.Mineur.Patch

1.3.5

5.2 MISES À JOUR DE SÉCURITÉ

Mises à jour de maintenance et correction de sécurité est automatique

5.3 MISES À JOUR DU CORE

Possibilité d'activé la màj automatique du core de
WordPress

Ajouter dans wp-config.php

```
define('WP_AUTO_UPDATE_CORE', true )
```

5.4 PLUGINS ET THEMES

Toujours mettre à jour les versions de patch

5.5 PHP MYSQL

Utiliser les dernières versions

Demander à votre hébergeur de faire les mјj et un
changelog

6. PLUGINS

Quelques plugins disponibles

6.1 PLUGINS

Wordfence <https://wordpress.org/plugins/wordfence/>

All in One WP Security & Firewall <https://wordpress.org/plugins/all-in-one-wp-security-and-firewall/>

iTheme Security Pro <https://wordpress.org/plugins/better-wp-security/>

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

SecuPress Free/Pro <https://wordpress.org/plugins/secupress/>

Sucuri Security <https://wordpress.org/plugins/sucuri-scanner/>

6.2 FAIRE LE MÉNAGE

Eviter de garder des plugins (et thèmes) qui ne sont pas utilisés.

QUESTIONS / EXPÉRIENCES

SOURCES ET RESSOURCES

Slides de Brigitte Djajasasmita: <https://www.bibiwordpress.ch/documents/20171012-SecuriteWordPress.pdf>

14 astuces pour sécuriser WordPress: <https://wpchannel.com/14-astuces-securiser-site-wordpress/>

Comment sécuriser votre site WordPress: <https://www.lafabriquedunet.fr/creation-site-vitrine/articles/tutoriel-comment-securiser-site-wordpress/>

Website Hacked Trend Report: <https://sucuri.net/website-security/website-hacked-report>

Ryan Markel: Security, the VIP Way: <https://wordpress.tv/2017/12/10/ryan-markel-security-the-vip-way/>

Sécuriser WordPress: <https://korben.info/securiser-wordpress-installation.html>

Authentification à deux facteurs pour une connexion WordPress: <https://www.wpnormandie.fr/authentification-a-deux-facteurs-pour-une-connexion-wordpress/>

A Complete Guide to WordPress Password Security: <https://premium.wpmudev.org/blog/a-complete-guide-to-wordpress-password-security/>

Two Step Authentication: https://codex.wordpress.org/Two_Step_Authentication

OBRIGADO

SUPERHUIT