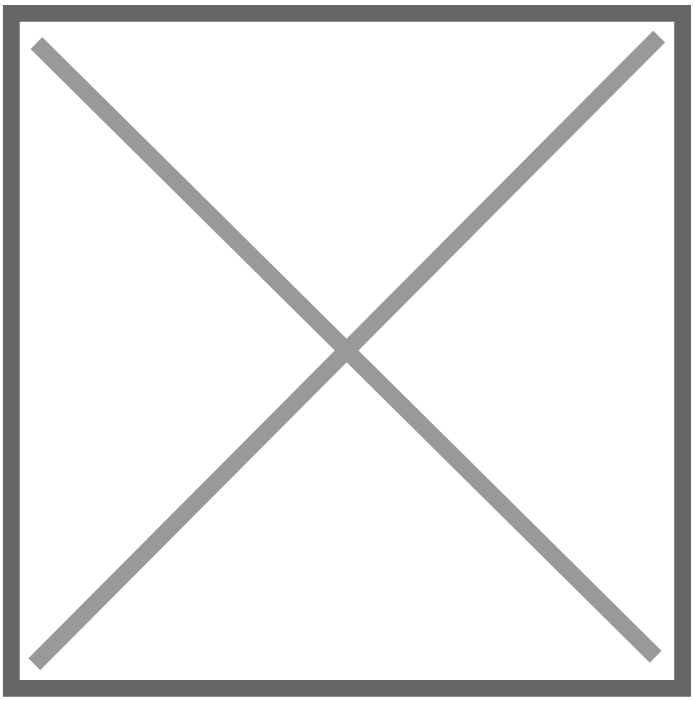
Sistemas de Administración de Contenidos (CMS)

Capítulo destinado a contenido relacionado a CMSs como ser wordpress, drupal, joomla y otros

- Guía de seguridad wordpress
- Guía de seguridad Joomla
- Enumeración de Usuarios en WordPress

Guía de seguridad wordpress



1. Introducción

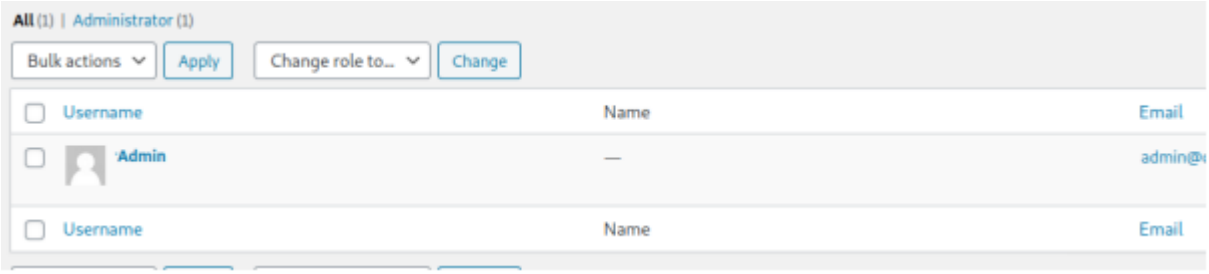
Wordpress es un sistema de gestión de contenido (CMS, Content Management System), que permite crear sitios web, su popularidad ha logrado que resulte muy atractivo para los “ciberatacantes”, con el fin de explotar vulnerabilidad

2. Asegurando Wordpress

Para mitigar el riesgo de ataques a Wordpress, recomendamos las siguientes buenas prácticas de seguridad.

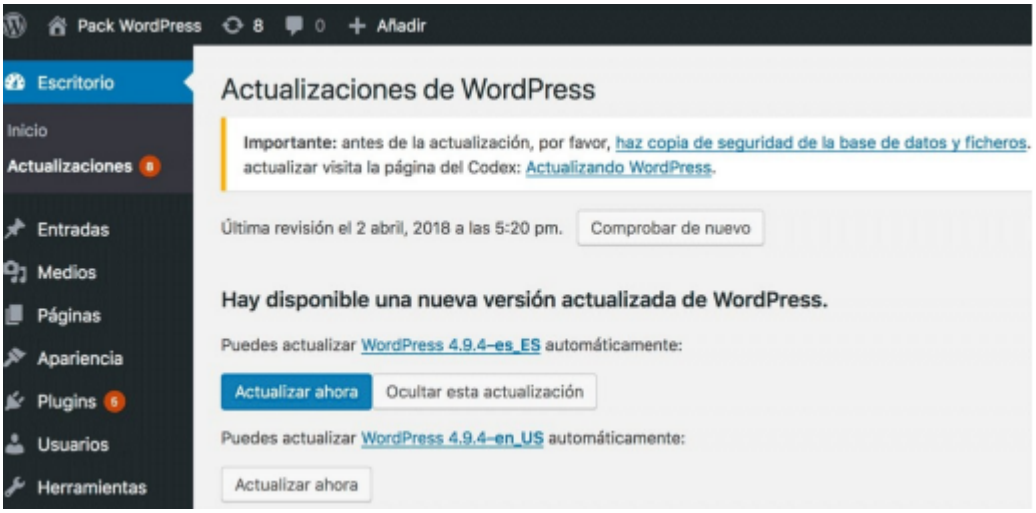
2.1. Configurar el control de acceso de usuarios

Ingresar al panel de administración de usuarios del sitio web: https://[midominio.gob.bo]/wp-admin/users.php y eliminar a los usuarios administradores que no se usan actualmente:



2.2. Actualizar el core de Wordpress

Ingresar a su sitio web https://[mi-dominio.gob.bo]/wp-admin/update-core.php y hacer click en el botón “Actualizar ahora”.

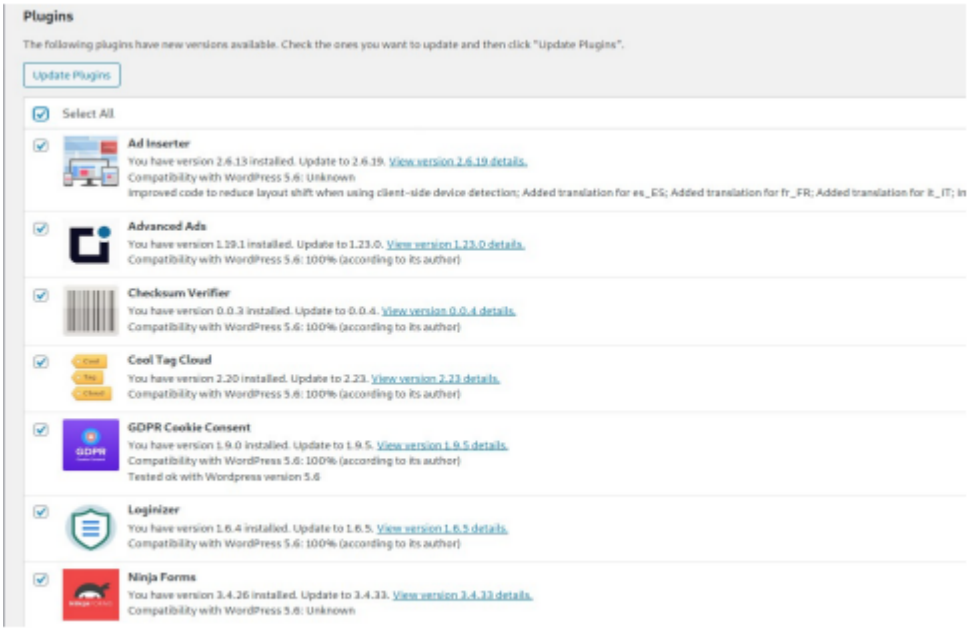


2.3. Actualizar los plugins de Wordpress

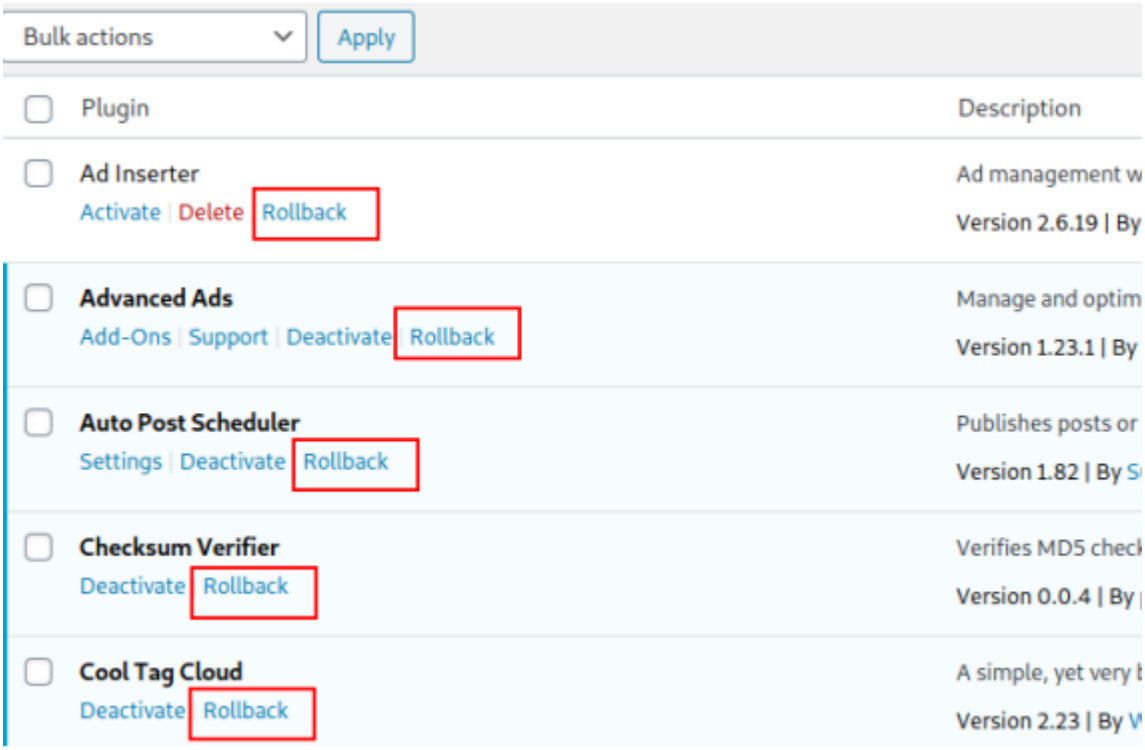
Previamente instalar y activar el plugin WP-Rollback (https://es.wordpress.org/plugins/wp-rollback/) que será útil en caso que la actualización de algún plugin no sea exitosa.

Realizar un backup de la base de datos.

Ingresar al sitio https://[mi-dominio.gob.bo]/wp-admin/update-core.php y seleccionar todos los plugins y presionar el botón “Actualizar plugins”.



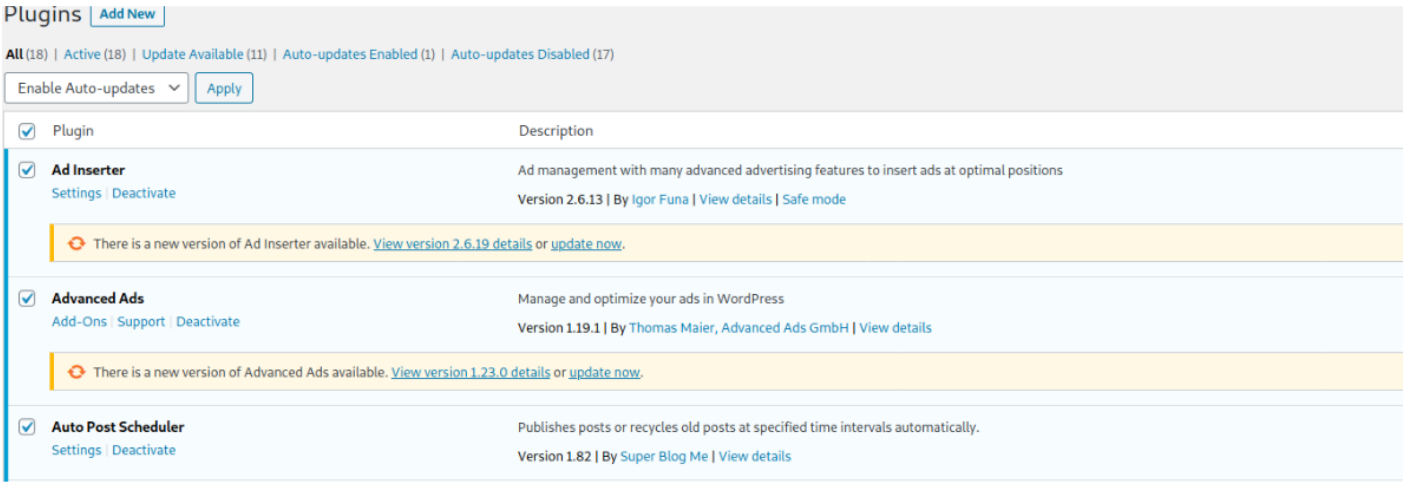
En caso de existir un error durante el proceso de actualización, realizar un ROLLBACK (https://[mi-dominio.gob.bo]/wp-admin/plugins.php).



2.4. Habilitar actualizaciones de seguridad automáticas

Ingresar al panel de administración https://[mi-dominio.gob.bo]/wp-admin/plugins.php y seleccionar todos los plugins.

Seleccionar la acción “habilitar actualizaciones automáticas” y ejecutar “Aplicar”



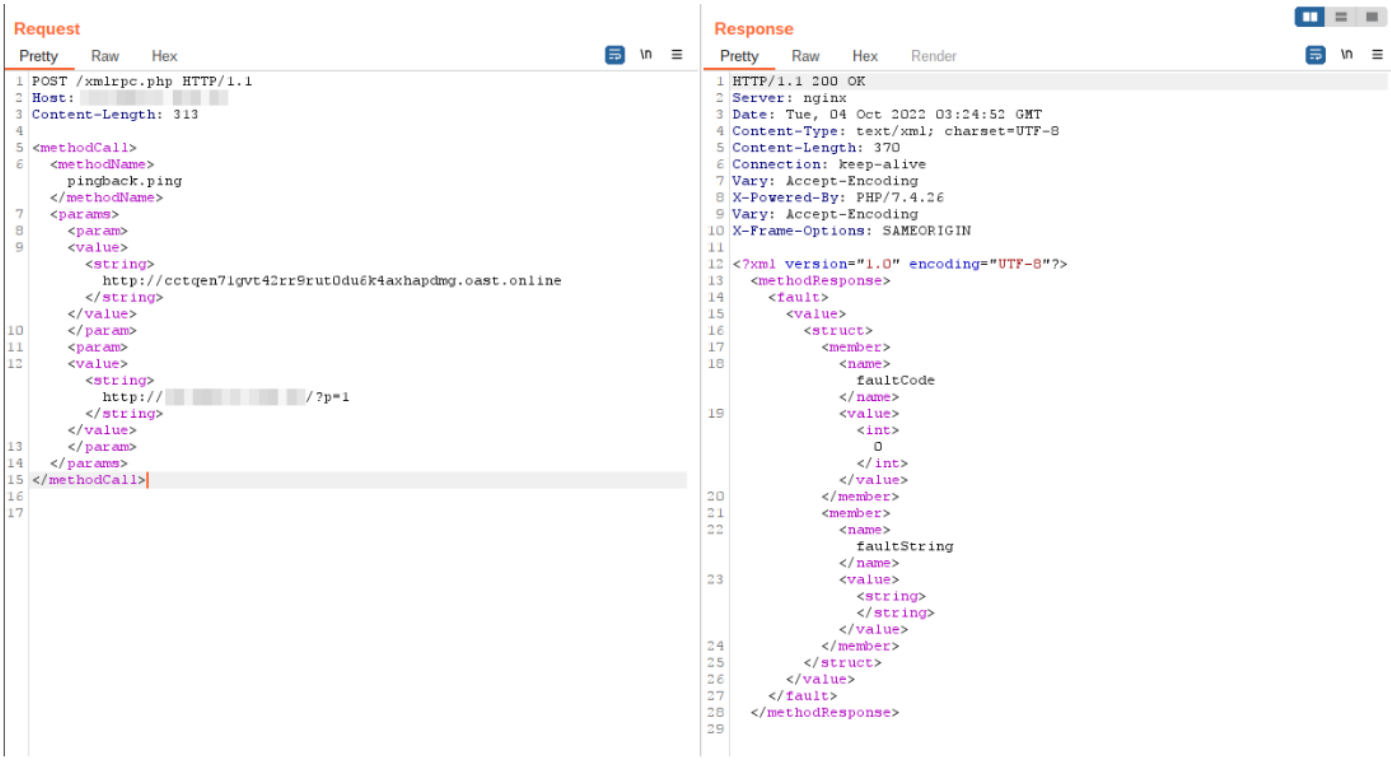
Borrar los themes no usados mediante la URL https://[mi-dominio.gob.bo]/wp-admin/themesphp

2.5. Deshabilitar XML-RPC

Wordpress tiene características para interactuar de forma remota con el sitio web, XML- RPC es una función de WordPress que permite la transmisión de datos con HTTP actuando como mecanismo de transporte y XML como mecanismo de codificación.

En la actualidad la funcionalidad del archivo xmlrpc.php ha disminuido considerablemente y su exposición y configuración insegura representa un riesgo en la seguridad del sitio web, provocando las siguientes vulnerabilidades:

- Ataques de fuerza bruta.
- Denegación Distribuida de Servicio.
- XMLRPC pingback.ping.



2.5.1. Restringir el acceso al archivo xmlrpc.php

Para restringir el acceso al archivo xmlrpc.php en apache2, se debe editar el archivo de configuración del sitio web o mediante el archivo .htaccess agregando las siguientes líneas:

```
<files xmlrpc.php>
order allow,deny
deny from all
</files>
```

Después reiniciar apache:

```
systemctl restart apache2
```

2.5.2. Deshabilitar la función XML-RPC

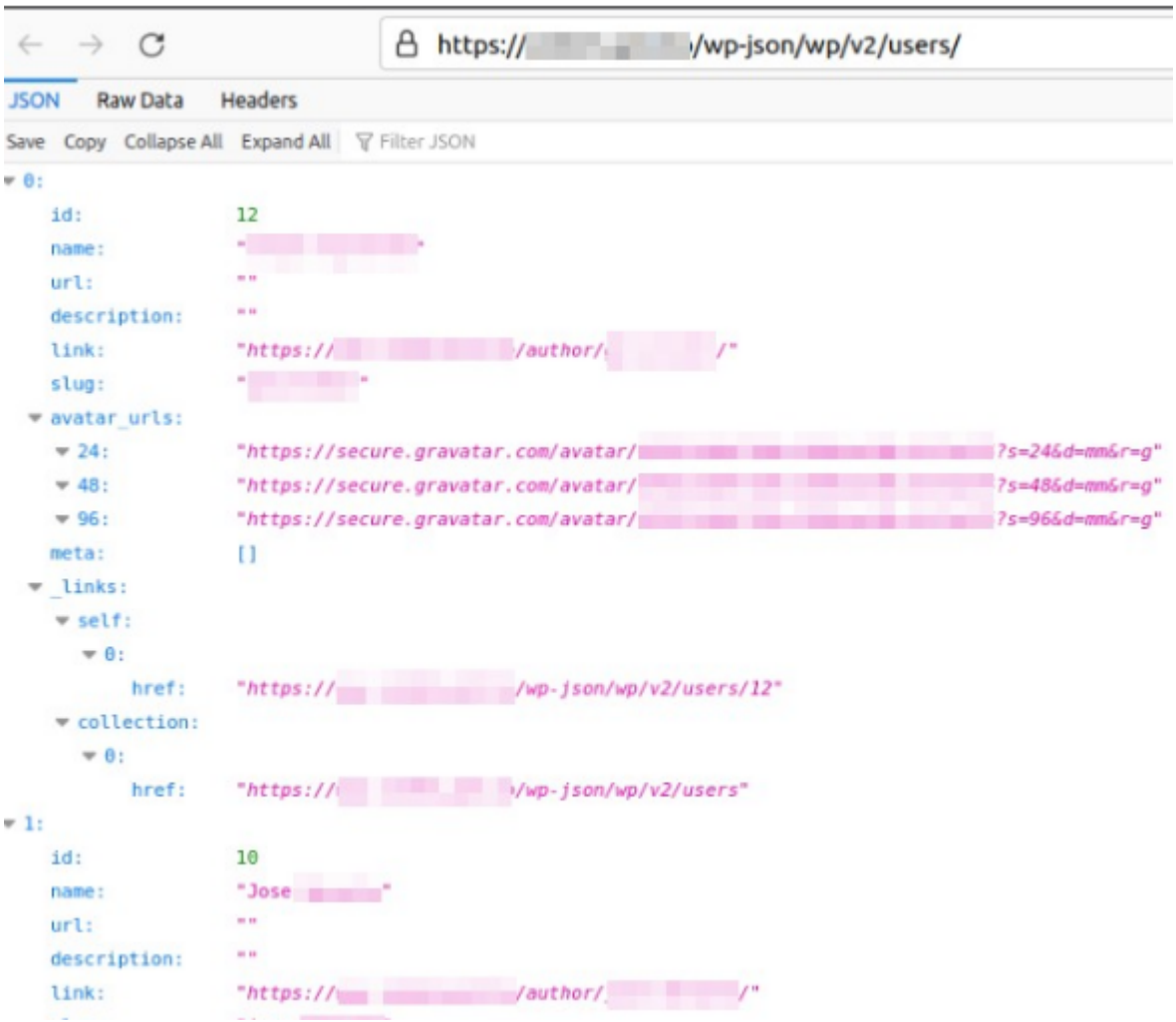
Si se determina que la función XML-RPC no es necesaria, se recomienda deshabilitarla, para ello se debe editar el archivo wp-config.php y agregar la siguiente línea:

```
add_filter('xmlrpc_enabled', '__return_false');
```

Otra opción para deshabilitar la función XML-RPC es instalando y activando el complemento “Disable XML-RPC”.

2.6. Enumeración de usuarios

Wordpress a través de su REST API puede exponer datos sensibles, como es el caso de los usuarios del sistema, si el sitio no está configurado de forma segura.



Para solucionar esta vulnerabilidad se debe actualizar a la versión 4.7.1 o posterior de Wordpress.

Una opción, en caso de no hacer uso del API REST de Wordpress, es deshabilitarlo, para ello se debe agregar las siguientes líneas en el archivo de configuración de wordpress wp-config.php:

```
add_filter('rest_enabled', '_return_false');
add_filter('rest_jsonp_enabled', '_return_false');
```

2.7. Utiliza contraseñas fuertes y seguras

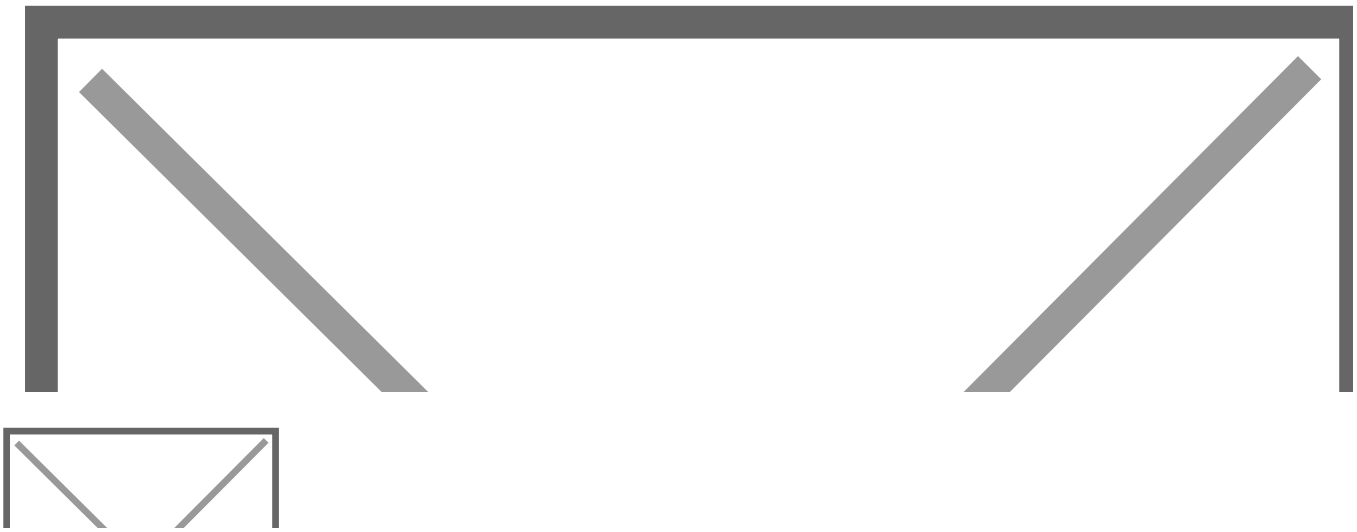
Utiliza contraseñas complejas y únicas para todas las cuentas de usuario, especialmente para los administradores.

Creación de Contraseñas

- **Longitud**: Usa contraseñas largas. Se recomienda al menos 12 caracteres, pero cuanto más larga, mejor.
- **Complejidad**: Incluye una combinación de letras mayúsculas y minúsculas, números y caracteres especiales como !, @, #, $, %, etc.
- **Evita Información Personal**: No uses información personal fácilmente disponible como nombres, fechas de nacimiento o números de teléfono.
- **Generación Segura**: Utiliza generadores de contraseñas para crear combinaciones aleatorias y seguras. Hay herramientas en línea y aplicaciones de administración de contraseñas que pueden ayudarte con esto.
- **Almacenamiento Seguro**: Usa administradores de contraseñas confiables para almacenar y gestionar contraseñas de forma segura.

En ese sentido en WordPress se debe seguir los siguientes pasos

- Inicia sesión en tu panel de administración de WordPress.
- Dirígete a "Usuarios" y luego a "Todos los usuarios".
- Haz clic en el nombre del usuario para el cual deseas cambiar la contraseña.
- Desplázate hacia abajo hasta la sección "Nueva contraseña".
- Ingresa una contraseña segura o utiliza el generador de contraseñas integrado haciendo clic en "Generar contraseña".
- Confirma la contraseña y guarda los cambios.



2.8 Implementa Autenticación de Dos Factores (2FA):

Usa un plugin de 2FA para añadir una capa adicional de seguridad a las cuentas de usuario.

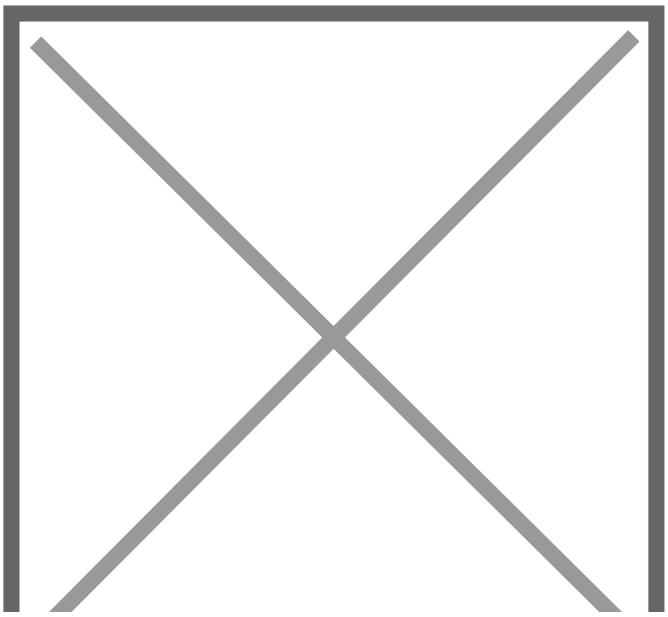
Autenticación de Dos Factores (2FA)

- **Segunda Capa de Seguridad**: Considera habilitar la autenticación de dos factores para agregar una capa adicional de seguridad más allá de la contraseña.

Pasos para Configurar 2FA en WordPress con Google Authenticator:

2.8.1. Instala un Plugin de 2FA:

- Dirígete a tu panel de administración de WordPress.
- Ve a **Plugins > Añadir nuevo**.
- Busca "Two Factor Authentication" o "Google Authenticator" y haz clic en **Instalar ahora**.



a. Activa el Plugin:

- Después de la instalación, haz clic en **Activar** para activar el plugin.

b. Configura el Plugin:

- Una vez activado, ve a **Usuarios > Perfil**.
- Desplázate hacia abajo hasta la sección de "Autenticación de dos factores".
- Selecciona "Habilitar la autenticación de dos factores para este usuario".

c. Configuración con Google Authenticator:

- Descarga e instala la aplicación "Google Authenticator" en tu dispositivo móvil desde la tienda de aplicaciones correspondiente (iOS o Android).

d. Escanea el Código QR:

- En la configuración de 2FA de tu perfil de WordPress, selecciona "Google Authenticator".
- Abre la aplicación Google Authenticator en tu teléfono y escanea el código QR que aparece en pantalla.
- Alternativamente, puedes introducir el código secreto manualmente si no puedes escanear el código QR.

e. Verificación:

- Una vez escaneado o introducido el código, la aplicación generará códigos de verificación de seis dígitos que cambian cada 30 segundos.
- Introduce el código de verificación generado por Google Authenticator en el campo correspondiente en tu perfil de WordPress.

f. Guarda los Cambios:

- Haz clic en **Actualizar perfil** para guardar la configuración.

g. Probar la Autenticación de Dos Factores:

- Cierra sesión en WordPress y vuelve a iniciar sesión.
- Introduce tu nombre de usuario y contraseña como de costumbre.
- Cuando se te solicite, abre la aplicación Google Authenticator en tu teléfono e introduce el código de verificación actual.

h. Configuración Adicional:

- Algunos plugins de 2FA permiten opciones adicionales, como la entrega de códigos por correo electrónico o SMS como método secundario de autenticación.

Para aplicar a todos los usuarios de tu sitio wordpress se debe activar la opción todos los usuarios como se ve en la siguiente imagen.

2.9. Limita los Intentos de Inicio de Sesión

Usa un plugin como "Limit Login Attempts Reloaded" para bloquear direcciones IP después de varios intentos fallidos de inicio de sesión.

Instalación de un Plugin de Seguridad:

- Busca y selecciona un plugin de seguridad confiable en WordPress, como "Limit Login Attempts Reloaded"
- Instalarlo y activarlo desde el panel de administración de WordPress.

Configuración del Plugin:

- Después de activar el plugin, ve a su configuración en el menú lateral de WordPress (generalmente bajo "Configuración" o "Seguridad").
- Encuentra la sección relacionada con la restricción de intentos de inicio de sesión.

Establecimiento de Límites y Acciones:

- Define el número máximo de intentos de inicio de sesión permitidos antes de que se active la restricción (por ejemplo, 3-5 intentos).
- Configura el tiempo de bloqueo de la dirección IP después de alcanzar el límite de intentos fallidos (por ejemplo, 15 minutos, 1 hora, etc.).

Personalización de Mensajes y Notificaciones:

- Algunos plugins te permiten personalizar los mensajes mostrados a los usuarios cuando exceden el límite de intentos de inicio de sesión.
- Configura notificaciones por correo electrónico o alertas dentro del panel de administración para informarte sobre intentos de inicio de sesión fallidos.

Prueba y Verificación:

- Realiza pruebas para asegurarte de que la restricción de intentos de inicio de sesión esté funcionando según lo esperado.

- Intenta iniciar sesión varias veces con credenciales incorrectas para verificar que se active la restricción después de alcanzar el límite establecido.

Monitoreo Continuo y Ajustes:

- Monitorea regularmente los registros de inicio de sesión y las alertas de tu plugin de seguridad para detectar actividades sospechosas.
- Ajusta la configuración según sea necesario para mantener un equilibrio entre seguridad y accesibilidad.

2.10. Cambia el Prefijo de la Base de Datos

Durante la instalación, cambia el prefijo predeterminado `wp_` de la base de datos a algo único para prevenir ataques SQL.

Cambiar el prefijo de la base de datos en WordPress es una medida de seguridad que puede ayudar a proteger tu sitio contra ataques SQL Injection. Aquí tienes una guía paso a paso para hacerlo:

Realizar una Copia de Seguridad Completa:

- Antes de realizar cualquier cambio en la base de datos, es crucial hacer una copia de seguridad completa de tu sitio web y de la base de datos.
- Puedes usar plugins como UpdraftPlus, BackupBuddy, o el propio sistema de backups de tu proveedor de hosting.

Desactivar Plugins de Caché y Seguridad:

- Desactiva temporalmente cualquier plugin de caché o seguridad para evitar conflictos durante el proceso.

Editar el Archivo `wp-config.php`:

- Accede al archivo `wp-config.php` en el directorio raíz de tu instalación de WordPress.

Encuentra la línea que define el prefijo de la base de datos, que generalmente se ve así:

Copiar código

```
$table_prefix = 'wp_';
```

Cambia el prefijo `wp_` a algo único, por ejemplo
Copiar código

```
$table_prefix = 'nuevo_prefijo_';
```

Actualizar el Prefijo en la Base de Datos:

- Usa una herramienta como phpMyAdmin o cualquier otro administrador de bases de datos para acceder a tu base de datos de WordPress.

Ejecuta las siguientes consultas SQL para cambiar el prefijo de todas las tablas
Copiar código

```
RENAME table `wp_commentmeta` TO `nuevo_prefijo_commentmeta`;

RENAME table `wp_comments` TO `nuevo_prefijo_comments`;

RENAME table `wp_links` TO `nuevo_prefijo_links`;

RENAME table `wp_options` TO `nuevo_prefijo_options`;

RENAME table `wp_postmeta` TO `nuevo_prefijo_postmeta`;

RENAME table `wp_posts` TO `nuevo_prefijo_posts`;

RENAME table `wp_terms` TO `nuevo_prefijo_terms`;

RENAME table `wp_termmeta` TO `nuevo_prefijo_termmeta`;

RENAME table `wp_term_relationships` TO `nuevo_prefijo_term_relationships`;

RENAME table `wp_term_taxonomy` TO `nuevo_prefijo_term_taxonomy`;

RENAME table `wp_usermeta` TO `nuevo_prefijo_usermeta`;

RENAME table `wp_users` TO `nuevo_prefijo_users`;
```

Actualizar las Referencias en la Base de Datos:

- Algunas tablas contienen referencias al prefijo antiguo. Debes actualizar estas referencias también. Ejecuta las siguientes consultas SQL

  Copiar código

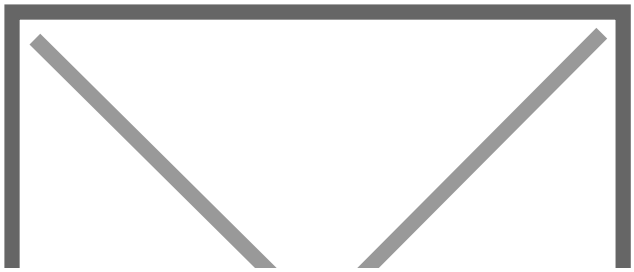
```
UPDATE `nuevo_prefijo_options` SET `option_name` = REPLACE(`option_name`, 'wp_', 'nuevo_prefijo_')
WHERE `option_name` LIKE 'wp_%';

UPDATE `nuevo_prefijo_usermeta` SET `meta_key` = REPLACE(`meta_key`, 'wp_', 'nuevo_prefijo_')
WHERE `meta_key` LIKE 'wp_%';
```

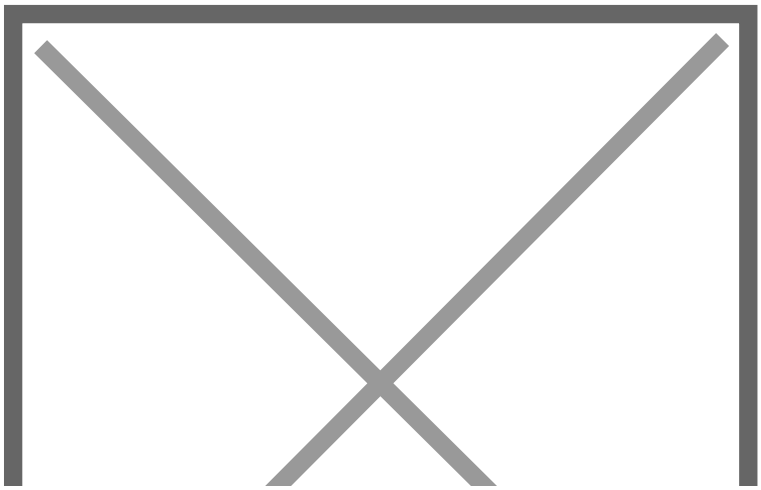
Verificar y Probar:

- Vuelve a activar los plugins de caché y seguridad.
- Revisa que todo esté funcionando correctamente en tu sitio web.
- Si encuentras algún problema, verifica las tablas y las referencias en la base de datos para asegurarte de que todas se han actualizado correctamente.

También se puede realizar utilizando el Plugins para cambiar el prefijo de la base de datos ayuda a reducir el riesgo de ataques automatizados que se aprovechan de la configuración predeterminada de WordPress. Esta medida, combinada con otras prácticas de seguridad, puede fortalecer significativamente la protección de tu sitio web

También se puede realizar mediante Plugin el cual describimos a continuación:
Desplegamos el Plugin





2.11 Oculta la Versión de WordPress:

Ocultar la versión de WordPress es una medida de seguridad que ayuda a proteger tu sitio de ataques dirigidos a vulnerabilidades específicas de la versión que estás utilizando. Aquí tienes una guía paso a paso para hacerlo:

2.11.1. Eliminar la Versión de WordPress del Código Fuente:

- Por defecto, WordPress añade la versión del sitio en el código fuente del HTML. Puedes eliminar esto añadiendo un pequeño fragmento de código en tu archivo `functions.php` .
- Ve al panel de administración de WordPress y navega a "Apariencia" > "Editor de temas" o accede a tu servidor mediante FTP y abre el archivo `functions.php` de tu tema activo.

Añade el siguiente código al archivo `functions.php`

Copiar código

```
// Eliminar la versión de WordPress del código fuente


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

2.11.2. Ocultar la Versión de WordPress en los Feeds RSS:

WordPress también incluye la versión del sitio en los feeds RSS. Para eliminar esto, añade el siguiente código al archivo `functions.php`:

Copiar códigoocultar

```
// Eliminar la versión de WordPress de los feeds RSS


function remove_wp_version_rss() {
```

```
    return '';

}

add_filter('the_generator', 'remove_wp_version_rss');
```

2.11.3. Eliminar la Versión de WordPress de los Scripts y Estilos:

Los scripts y estilos en WordPress a menudo tienen la versión de WordPress adjunta. Puedes eliminar esto añadiendo el siguiente código al archivo `functions.php`.
Copiar código

```
// Eliminar la versión de WordPress de los scripts y estilos

function remove_wp_version_scripts_styles($src) {

    if (strpos($src, 'ver=')) {

        $src = remove_query_arg('ver', $src);

    }

    return $src;

}

add_filter('style_loader_src', 'remove_wp_version_scripts_styles', 9999);

add_filter('script_loader_src', 'remove_wp_version_scripts_styles', 9999);
```

Verificar la Implementación:

- Después de realizar estos cambios, verifica que la versión de WordPress no sea visible en el código fuente de tu sitio.
- Abre tu sitio en un navegador, haz clic derecho y selecciona "Ver código fuente de la página" (o similar según el navegador).

Busca cualquier mención de la versión de WordPress. Si la has eliminado correctamente, no deberías encontrarla.

Implementar estas medidas ayuda a reducir el riesgo de que los atacantes exploten vulnerabilidades específicas de tu versión de WordPress, aumentando así la seguridad general de tu sitio web

2.12. Usa HTTPS/SSL:

Asegúrate de que tu sitio web utiliza HTTPS instalando un certificado SSL.

1. Uso de Certificados SSL.

Aquí tienes los pasos simplificados para instalar un certificado SSL en WordPress:

2. Obtener un Certificado SSL:

a. Puedes obtener un certificado SSL a través de tu proveedor de hosting. Algunos proveedores ofrecen certificados SSL gratuitos a través de servicios como Let's Encrypt.

3. Instalar el Certificado SSL:

a. En tu panel de control de hosting, busca la sección de SSL o certificados.

b. Activa o instala el certificado SSL proporcionado por tu proveedor. Sigue las instrucciones específicas de tu proveedor de hosting para completar la instalación del certificado SSL en tu dominio.

4. Actualizar la URL de WordPress a HTTPS:

a. Inicia sesión en el panel de administración de WordPress.

b. Ve a "Ajustes" > "General".

c. Actualiza las direcciones URL de WordPress a HTTPS en los campos "Dirección de WordPress

5. Redireccionar HTTP a HTTPS (opcional pero recomendado):

a. Para asegurarte de que todas las páginas carguen a través de HTTPS, puedes configurar redirecciones desde HTTP a HTTPS.

b. Esto se puede hacer mediante el archivo .htaccess en Apache, o a través de la configuración del servidor si estás usando Nginx u otro servidor web.

3. **Verificar el Funcionamiento del SSL:**

   a. Una vez configurado, verifica que tu sitio web cargue correctamente utilizando HTTPS.

   b. Comprueba que no haya advertencias de seguridad y que el candado verde o el icono de seguridad se muestren en la barra de direcciones del navegador.

4. **Actualizar Enlaces Internos y Contenido Mixto (si es necesario):**

   a. Si tu sitio web contiene enlaces internos con URLs absolutas (HTTP), actualízalos a HTTPS.

   b. Verifica que no haya contenido mixto (elementos HTTP en una página HTTPS), ya que pueden causar advertencias de seguridad en los navegadores.

5. **Configurar Recursos de Seguridad Adicionales (opcional):**

   a. Considera configurar políticas de seguridad HTTP como Content Security Policy (CSP) para mejorar la seguridad de tu sitio web.

   b. Implementa encabezados HTTP estrictos para proteger contra ataques como XSS y Clickjacking.

2.13. Usa Google reCAPTCHA

Añade Google reCAPTCHA a tus formularios de inicio de sesión, registro y comentarios para evitar el spam y los intentos de inicio de sesión automatizados.

1. **Instalar un Plugin de CAPTCHA:**
   - Ve al panel de administración de WordPress.
   - Navega a "Plugins" > "Añadir nuevo".
   - Busca un plugin de CAPTCHA. Algunas opciones populares incluyen "reCAPTCHA by BestWebSoft", "Google Captcha (reCAPTCHA) by BestWebSoft" y "WP-reCAPTCHA".
4. **Instalar y Activar el Plugin:**
   - Haz clic en "Instalar ahora" junto al plugin de tu elección.
   - Una vez instalado, haz clic en "Activar".
3. **Configurar el Plugin de CAPTCHA:**
   - Después de activar el plugin, generalmente encontrarás una nueva opción en el menú lateral del panel de administración, como "reCAPTCHA" o "Google Captcha".
   - Navega a la página de configuración del plugin.
3. **Obtener las Claves de reCAPTCHA:**
   - Si estás utilizando Google reCAPTCHA, necesitarás obtener las claves del sitio y secreto desde Google reCAPTCHA.

- Regístrate en Google reCAPTCHA con tu cuenta de Google, añade tu sitio web y obtén las claves necesarias.

3. **Configurar las Claves en el Plugin:**

- Ingresa las claves del sitio y secreto en los campos correspondientes en la página de configuración del plugin.
- Configura las opciones adicionales según tus necesidades, como en qué formularios deseas habilitar el CAPTCHA (inicio de sesión, registro, comentarios, etc.).

3. **Guardar la Configuración:**

- Guarda los cambios realizados en la configuración del plugin.

2. **Verificar la Implementación del CAPTCHA:**

- Visita las páginas de inicio de sesión, registro o comentarios de tu sitio web para asegurarte de que el CAPTCHA esté correctamente implementado.
- Realiza pruebas para confirmar que el CAPTCHA está funcionando como se espera y que no afecta la usabilidad del sitio para los usuarios legítimos.

3. **Monitorear y Ajustar:**

- Monitorea el rendimiento del CAPTCHA y ajusta la configuración si es necesario para mejorar la protección contra bots y spam sin afectar negativamente la experiencia del usuario.

2.14. Configuración de Copias de Seguridad Automáticas.

Instala un Plugin de Copias de Seguridad:

- En el panel de administración de WordPress, ve a "Plugins" y luego a "Añadir nuevo".
- Busca un plugin de copias de seguridad como UpdraftPlus, BackupBuddy o VaultPress.
- Instala y activa el plugin elegido.

Configura el Plugin de Copias de Seguridad:

- Después de activar el plugin, debería aparecer en el menú lateral de WordPress.
- Haz clic en el nombre del plugin para acceder a su configuración.

Crea un Nuevo Trabajo de Copia de Seguridad:

- Dentro del plugin, busca la opción para crear una nueva copia de seguridad o configurar un nuevo trabajo de copia de seguridad.

Selecciona Qué Incluir en la Copia de Seguridad:

- Elige si deseas incluir la base de datos de WordPress, los archivos del sitio, o ambos.
- Algunos plugins te permiten seleccionar automáticamente los archivos y la base de datos necesarios.

Configura la Frecuencia y Horario:

- Define la frecuencia de las copias de seguridad automáticas (diariamente, semanalmente, mensualmente) y el horario en que deseas que se realicen.

Elige el Destino de la Copia de Seguridad:

- Decide dónde almacenar las copias de seguridad. Puedes usar servicios de almacenamiento en la nube como Dropbox, Google Drive, Amazon S3, o almacenamiento local en el servidor.

Configura Opciones Avanzadas (si es necesario):

- Algunos plugins ofrecen opciones avanzadas como compresión de archivos, cifrado de copias de seguridad, exclusión de archivos específicos, etc. Configura según tus necesidades.

Guarda y Activa el Trabajo de Copia de Seguridad:

- Una vez configurado, guarda la configuración y activa el trabajo de copia de seguridad. Asegúrate de que esté programado según tus preferencias.

Prueba y Verifica:

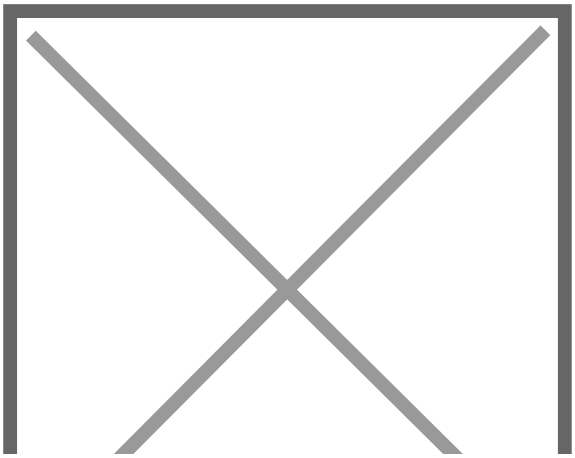
- Realiza una prueba inicial para asegurarte de que las copias de seguridad automáticas se están realizando correctamente.
- Verifica que los archivos y la base de datos se estén respaldando como esperabas.

Monitoriza y Mantén:

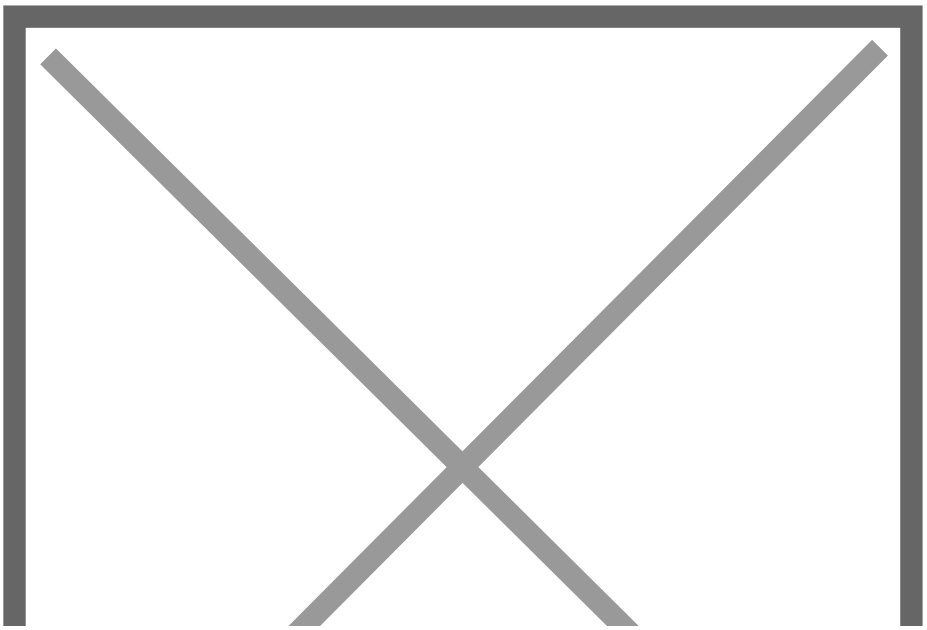
- Supervisa regularmente las copias de seguridad automáticas para asegurarte de que se estén realizando correctamente.
- Ajusta la configuración según sea necesario para mantener la seguridad y la disponibilidad de las copias de seguridad.

2.15. Crea Copias de Seguridad Regularmente:

Usa plugins como UpdraftPlus o BackWPup para crear copias de seguridad regulares de tu sitio.
Se puede realizar mediante plugin



En la parte de ajustes dentro del plugins



Guía de seguridad Joomla

1. Introducción

Joomla es un sistema de gestión de contenido (CMS, Content Management System), que permite crear sitios web, su popularidad ha logrado que resulte muy atractivo para los actores maliciosos, con el fin de explotar vulnerabilidades.

2. Asegurando joomla

Para mitigar el riesgo de ataques a Joomla, se recomiendan las siguientes buenas prácticas de seguridad.

2.1. Verificar parches de seguridad

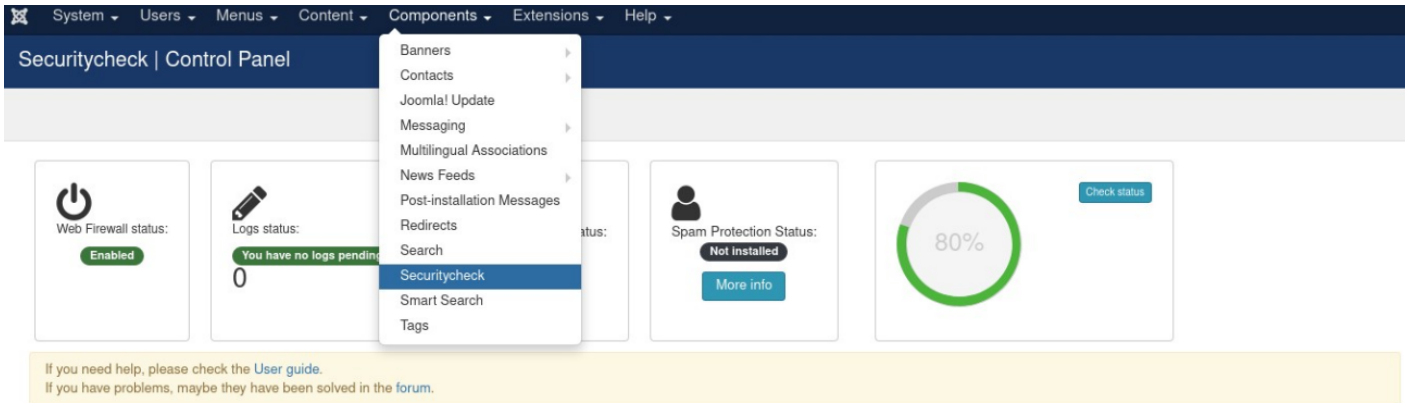
Comprobar regularmente si hay nuevos parches de seguridad disponibles para solucionar vulnerabilidades de seguridad e instalarlos, para ello existe el complemento “Plugin Securitycheck”.

A continuación se describe los pasos para el uso del Plugin Securitycheck:

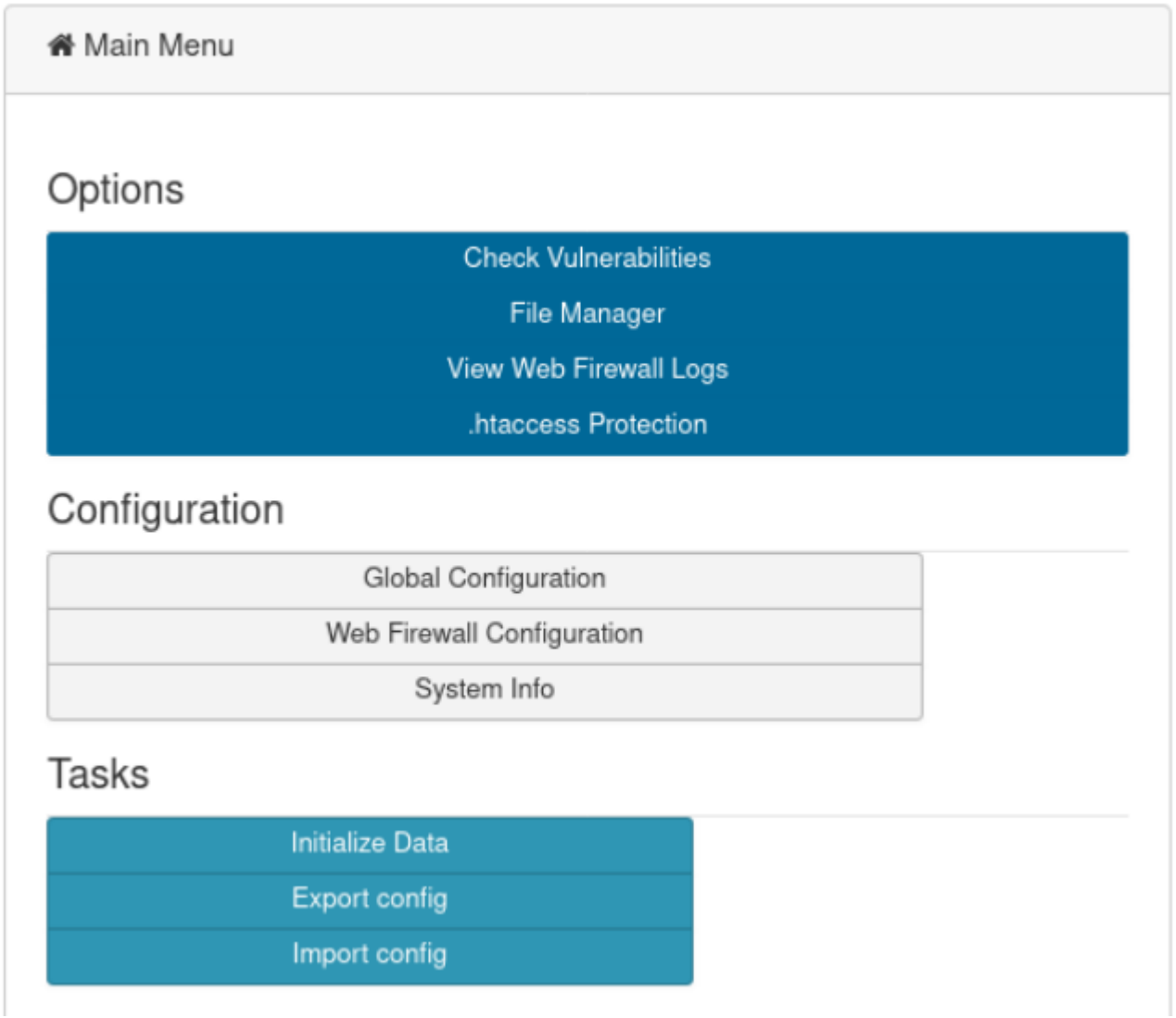
- Instalar el plugin siguiendo el enlace:

  https://extensions.joomla.org/extension/securitycheck/

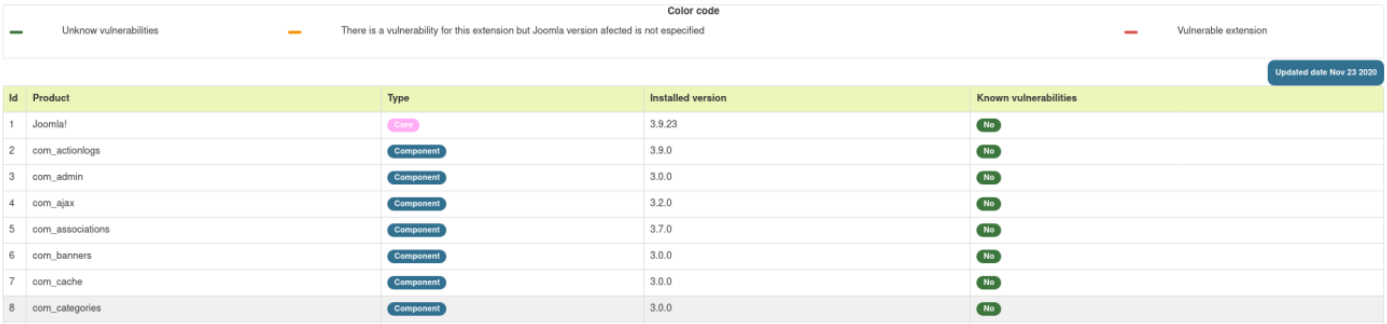
- Una vez instalado ir al menú Components→Securitycheck



- Verificar vulnerabilidades en los complementos.



- La columna de “Known vulnerabilities” de todos los complementos listados debe estar en estado “No”.



Se recomienda suscribirse a canales de seguridad oficiales de Joomla, por ejemplo:

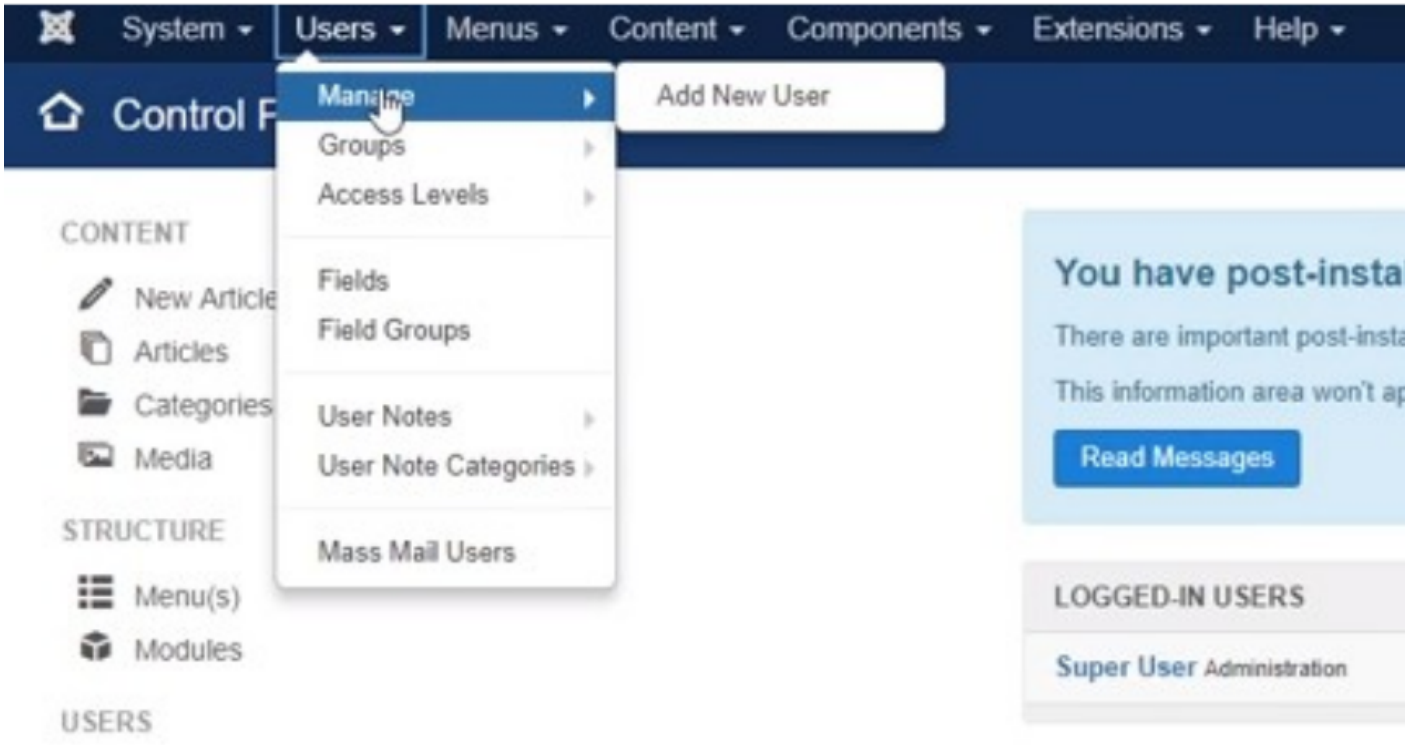
- https://docs.joomla.org/Security_hotfixes_for_Joomla_EOL_versions/es
- https://developer.joomla.org/security-centre.html

Siempre debe mantener actualizado Joomla a una versión con soporte.

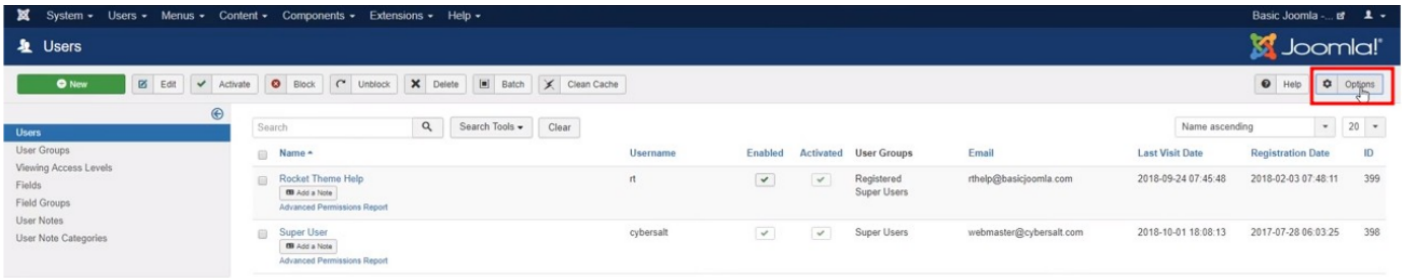
También se recomienda que se considere actualizar las tecnologías complementarias para el uso de Joomla como es php, mysql y el sistema operativo, tomando en cuenta que estas actualizaciones sean compatibles con la versión de Joomla que utiliza, aplicando estos cambios primero en un entorno de pruebas.

2.2. Asegurar nombre de usuario y contraseña

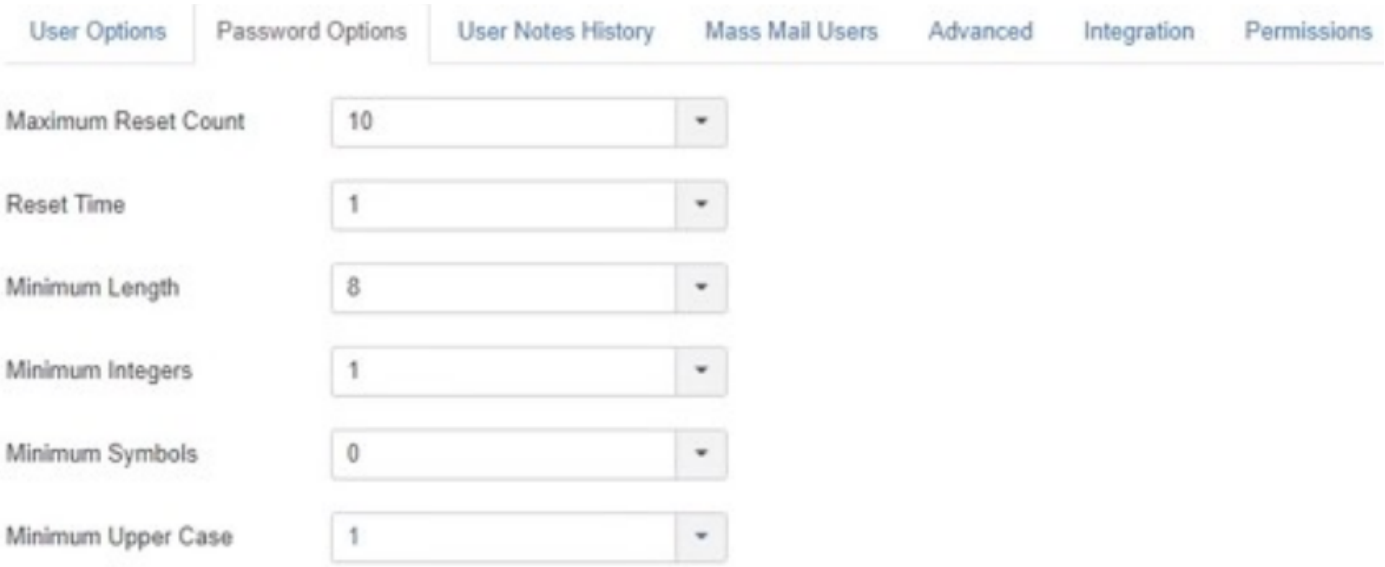
- No utilizar el nombre de usuario admin predeterminado.
- Utilizar una contraseña robusta, por ejemplo, que contenga mayúsculas, minúsculas, cifras y caracteres especiales.
- Configurar la robustez de la contraseña, para ello se debe ingresar a Users > Manage:



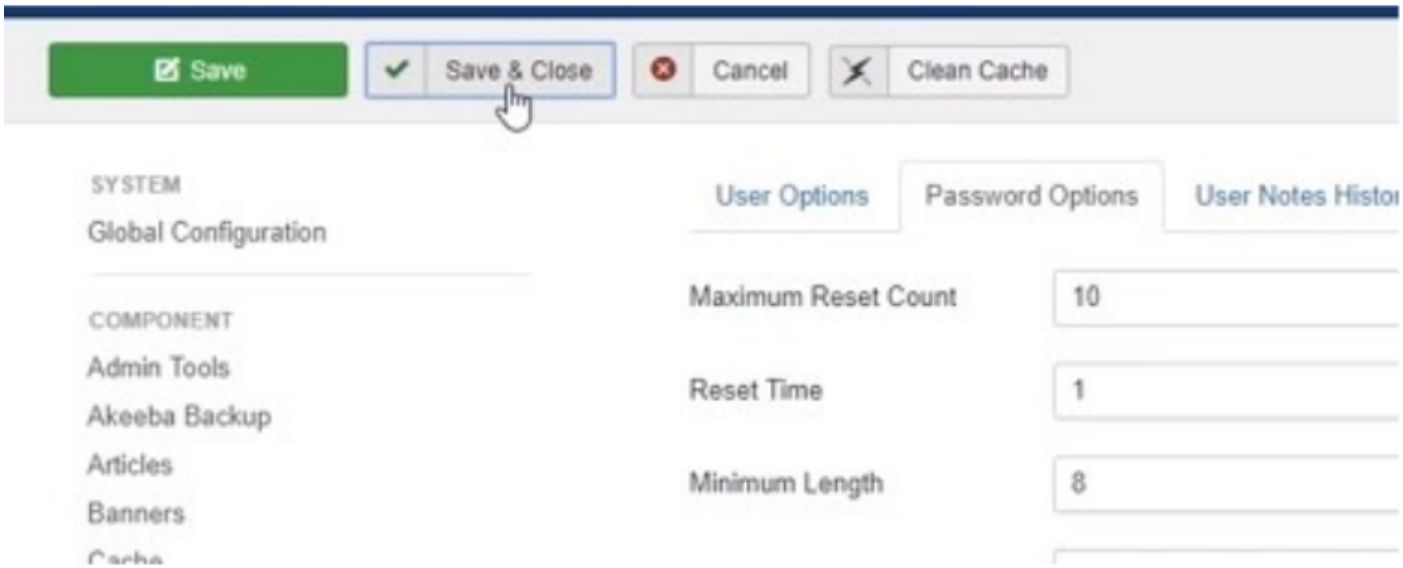
- Seleccionar Options:



- En password options establecer:



- Guardar y cerrar:



2.3. Proteger el archivo de configuración

Proteger el archivo configuration.php, que se encuentra en el directorio raíz de la instalación de Joomla con apache, para impedir que se pueda editar.

- Activar el módulo htaccess:

```
$ sudo nano /etc/apache2/apache2.conf
```

- Buscar las líneas:

```
<Directory /var/www/>
	Options Indexes FollowSymLinks
	AllowOverride None
	Require all granted
</Directory>
```

Cambiar a:

```
<Directory /var/www/>
	Options FollowSymLinks
	AllowOverride All
	Require all granted
</Directory>
```

- Reiniciar servidor de apache:

```
$ sudo service apache2 restart
```

- Añadir al archivo .htaccess:

```
<FilesMatch “configuration.php”>
	Require all denied
</FilesMatch>
```

- Cambiar los permisos considerando:

  Archivos PHP - 644
  Archivos de configuración - 644
  configuration.php: 440
  Otras carpetas - 755

2.4. Proteger el acceso al panel de administrador

Por defecto el panel de administrador de Joomla se encuentra en la url “/administrator” de la página. Para evitar que personas no autorizadas intenten acceder al panel de administración seguir los siguientes pasos:

- Crear un directorio que únicamente conozcan los usuarios administradores del sitio web (debe recordar que el directorio miotroadm es solo un ejemplo).

```
$ sudo mkdir miotroadm
```

- Crear un archivo index.php para redireccionar al panel de administración, cambiar la cookie “admin_cookie_code” por una más larga y difícil de adivinar.

```
$ cd miotroadm
$ sudo nano index.php
```

```
<?php
$admin_cookie_code="1254789654258"
setcookie("JoomlaAdminSession",$admin_cookie_code,0,"/");
header("Location: ../administrator/index.php");
?>
```

- Adicionar al principio del index.php del directorio “administrator” que solicite la cookie, caso contrario devolver al index.php

```
$ sudo nano administrator/index.php
```

```
if($_COOKIE['JoomlaAdminSession']!="1254789654258")
{
setcookie('JoomlaAdminSession', null, -1, '/');
header("Location: ../../index.php");
}
```

- Añadir al final en el index.php del panel de administración el siguiente comando para eliminar la cookie creada.

```
$ sudo nano index.php
```

```
if ($_COOKIE['JoomlaAdminSession']!="")
{
setcookie('JoomlaAdminSession', null, -1, '/');
}
```

2.5. Ocultar la versión de Joomla

Deberá deshabilitar manualmente ingresando al panel de administración de joomla:

Site > Global Configuration

Establecer en “No” la opción “Show Joomla Version”.

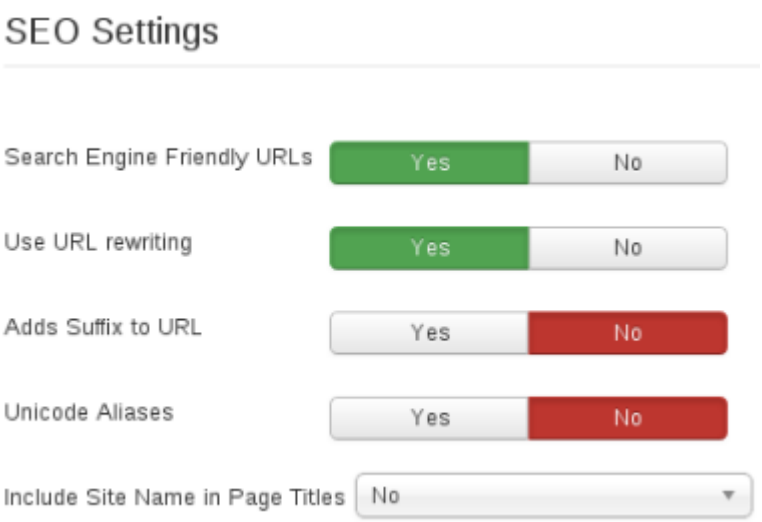
Adicionalmente, deberá eliminar la carpeta “installation” ubicada en el directorio raíz de la instalación de Joomla.

2.6. Activar search engine friendly (sef)

SEF permite hacer las URLs de Joomla más amistosas para el usuario y también dificulta a los escáneres automatizados encontrar información útil para efectuar ataques al sitio web.

Para activar SEF en Joomla debe acceder al panel de administración e ingresar a “Global Configuration”.

Establecer la opción Search Engine Friendly URLs en “Yes”:



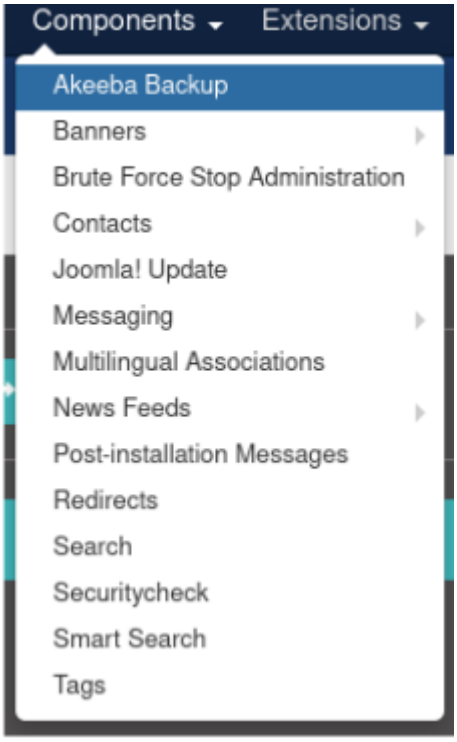
2.7. Realizar copia de seguridad

Para realizar la copia de seguridad de Joomla puede utilizar el plugin Akeeba Backup.

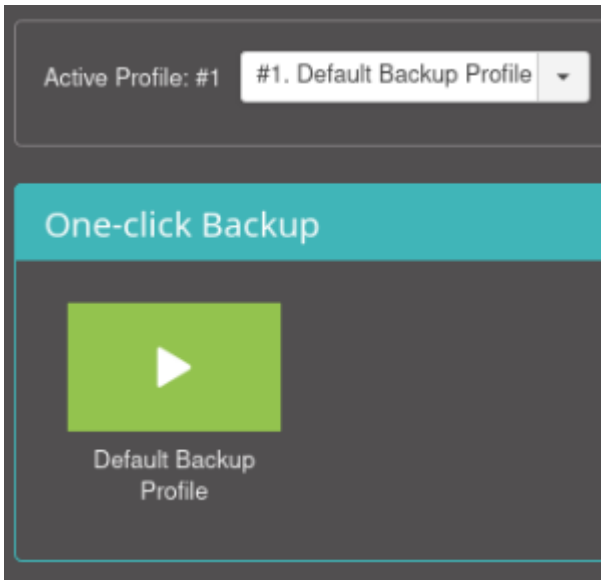
- Instalar el plugin siguiendo el enlace:

  https://extensions.joomla.org/extension/akeeba-backup/

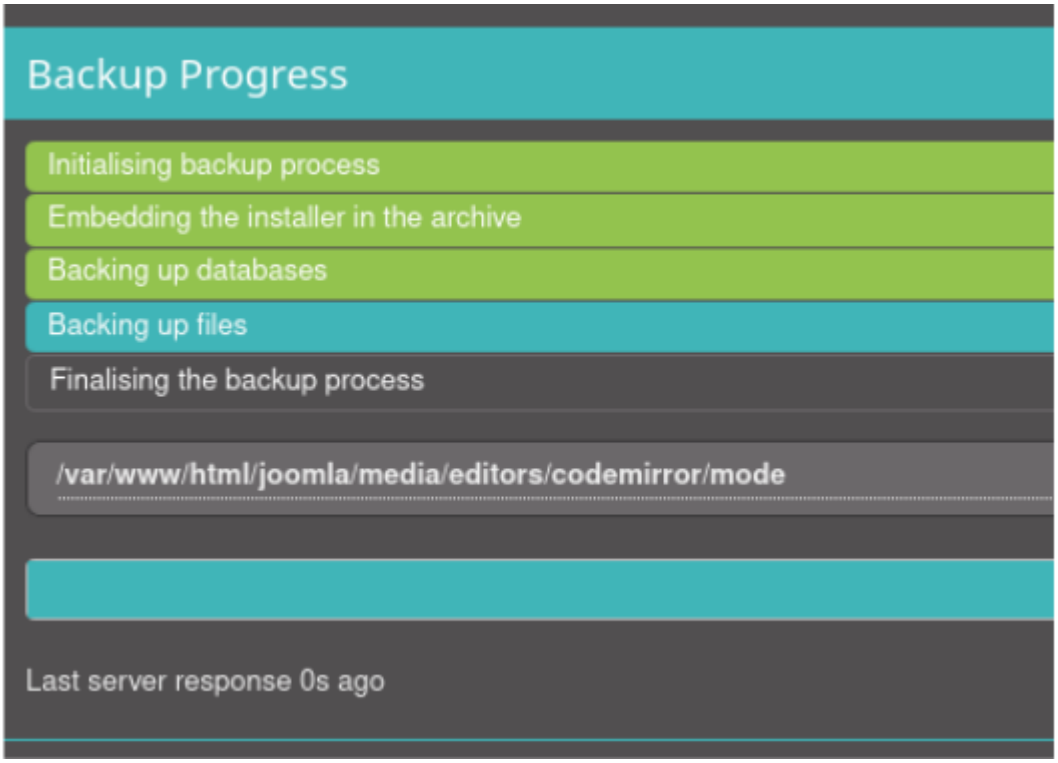
- Una vez instalado ir al menú Components>Akeeba Backup



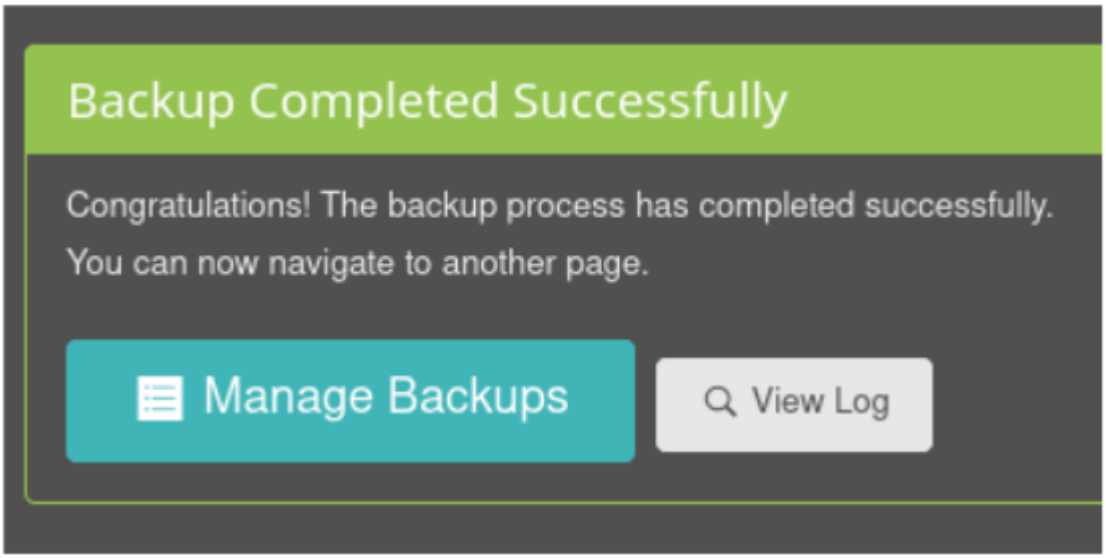
- Hacer clic en “Default Backup Profile” para sacar la copia de seguridad de Joomla.



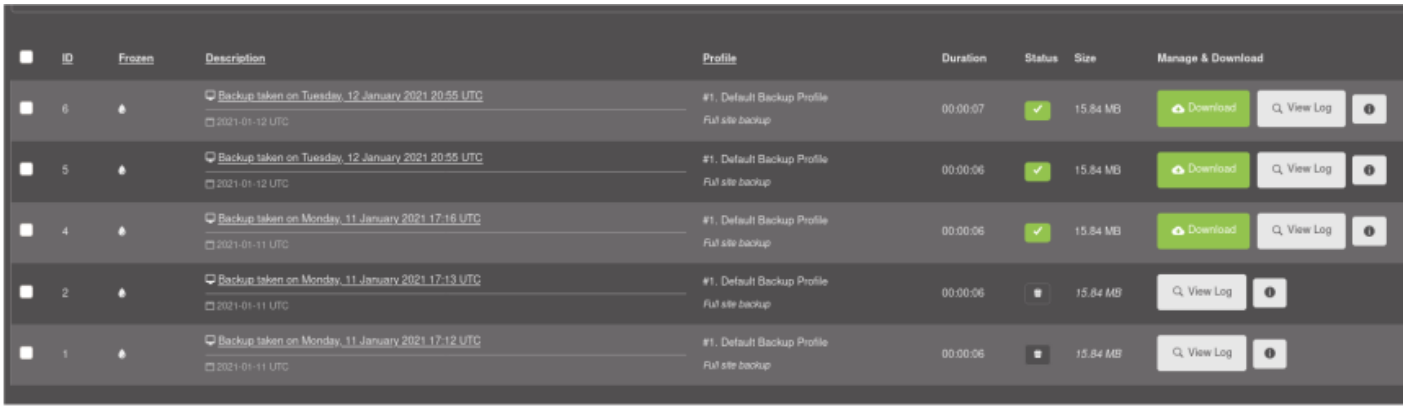
- Se despliega el proceso de backup



- Los backups se muestran en Manage Backups.



- Se muestra el listado de backups generados.



- Establecer copias de respaldo cada cierto tiempo de acuerdo a las políticas de seguridad.

Enumeración de Usuarios en WordPress

¿Qué es la enumeración de usuarios?

La enumeración de usuarios, es una forma de obtener datos de usuarios de su sitio web a través de scripts maliciosos. Aunque el pirata informático solo puede obtener los detalles del nombre de usuario con esto, sigue siendo un riesgo grave. Conocer el nombre de usuario es la mitad del trabajo realizado por un pirata informático al ejecutar un ataque de fuerza bruta.

Método 1: Archivos de autor

Quizás el método más fácil para encontrar nombres de usuario de WordPress es revisar los archivos del autor. Para enumerar nombres de usuario a través del método de archivos del autor. Para enumerar nombres de usuario a través del método de archhivos de autor, simplemente agregue un número entero (es decir: 1,2,3,etc.) como valor al parámetro "autor". Por ejemplo:

- https://tusitio.com/?author=1
- https://tusitio.com/?author=2
- https://tusitio.com/?author=3

Estos valores luego obtendrían resultados como los siguientes:

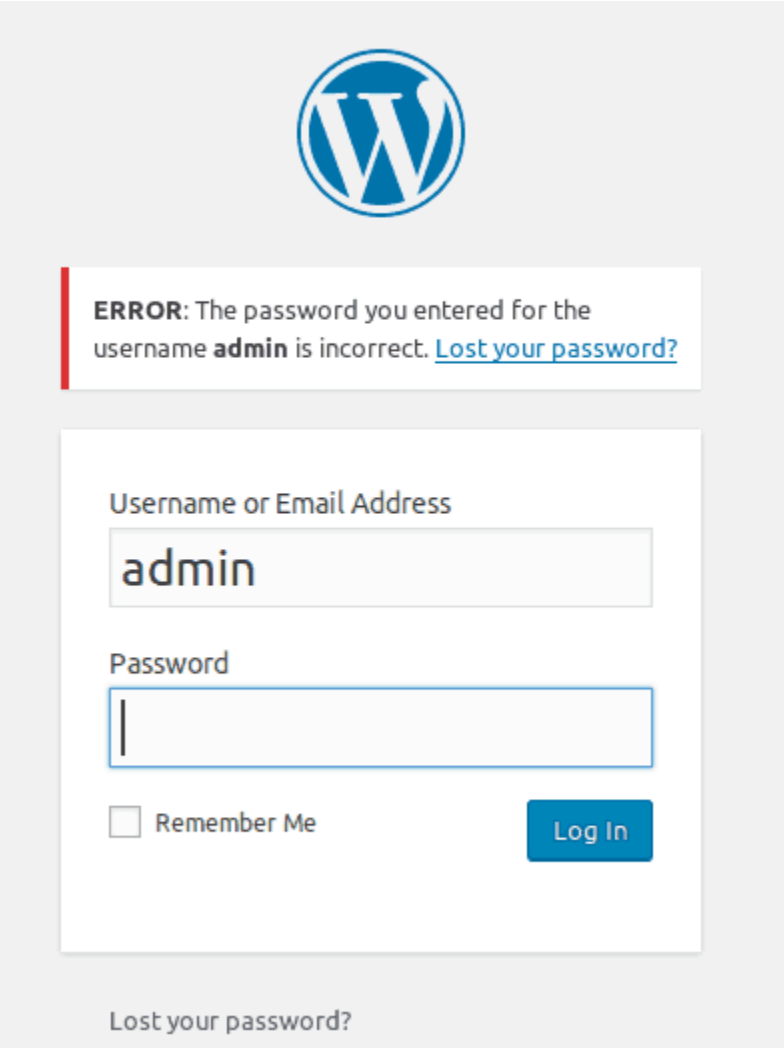
- https://tusitio.com/author/admin/
- https://tusitio.com/author/user2/
- https://tusitio.com/author/user3/

Por lo tanto, al confundir el autor del parámetro en la URL de inicio de WordPress, se pueden enumerar varios nombres de autor.

Método 2: Mensajes de error

A veces, el atacante intenta iniciar sesión en su sitio de WordPress con un nombre de usuario aleatorio. Si el nombre de usuario existe, el mensaje de error revelará que el nombre de usuario es correcto pero la contraseña es incorrecta. De manera similar, si el nombre de usuario adivinado es

incorrecto, el mensaje de error especificaría que el nombre de usuario no existe. Ahora, al utilizar el enfoque de fuerza bruta, el atacante puede enumerar nombres de usuario en función de los mensajes de error.



El mensaje de error revela el nombre de usuario como "admin" se encuentra registrado como usuario del sistema.

Solución a la enumeración de usuarios

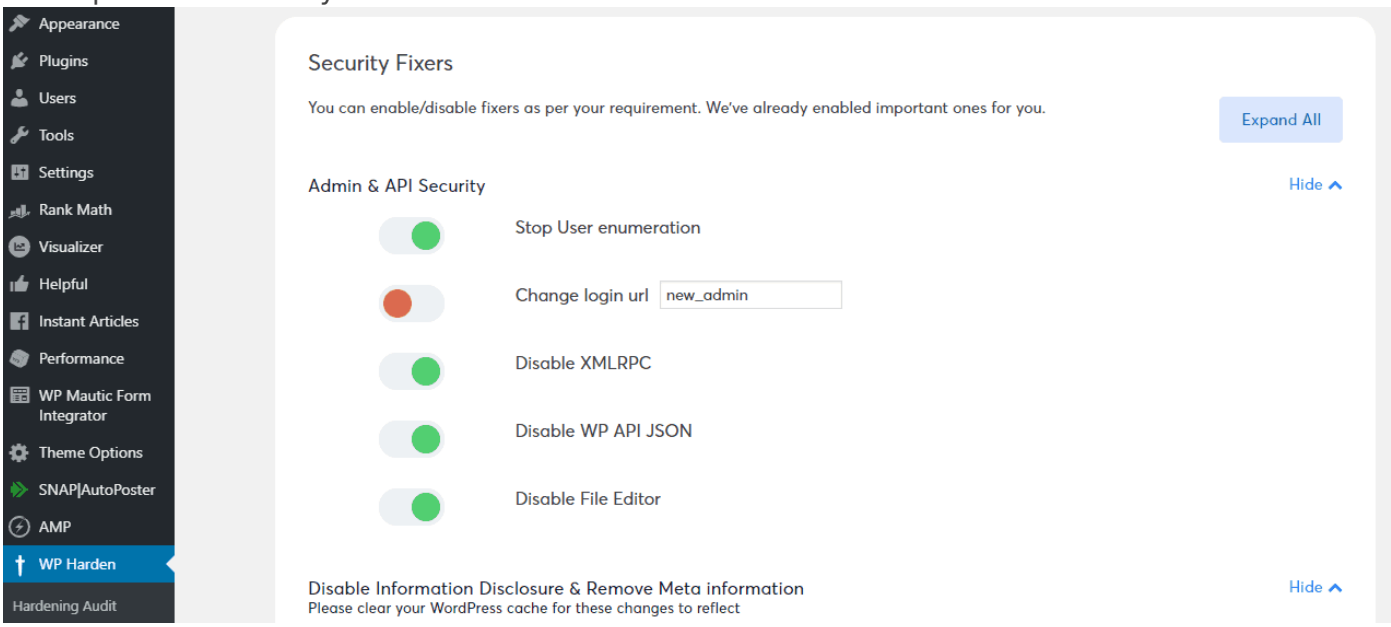
Aplique una de las siguientes opciones para evitar la enumeración de usuarios en WordPress (preferente la opción 1):

1. Instalación de WP-Hardening

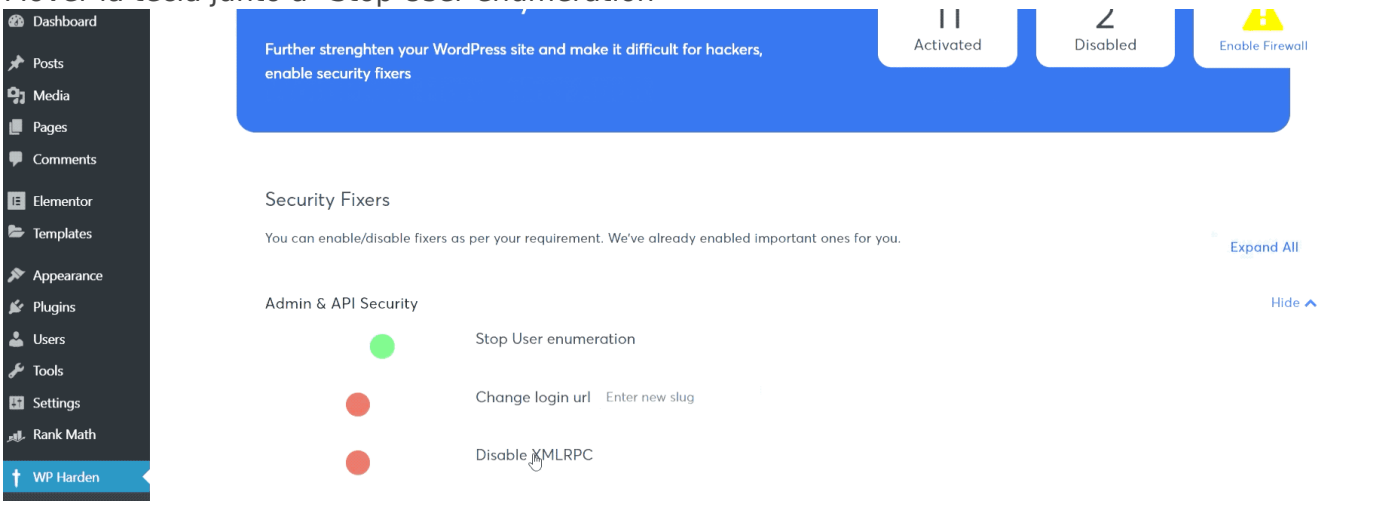
1. Instalar y activar el complemento.
    1. Ir a ‘Plugins > Add New’ en el panel de administración.
    2. Buscar ‘WP-Hardening’
    3. Instalar WP-Hardening una vez que aparezca.

4. Activarlo desde su página Plugins.
5. El botón WP-Hardening aparecerá en la parte inferior izquierda de su panel de administración.

2. Ir a la pestaña 'Security Fixers'



3. Mover la tecla junto a "Stop User enumeration"



2. Editando archivos de WordPress

Agregando un fragmento de código al archivo functions.php o al archivo .htaccess en el nivel raíz. El archivo .htaccess debe editarse solo si desea bloquear la solicitud a nivel del servidor.

Método 1: Modificar el archivo functions.php.

- Paso 1: Inicie sesión en el panel de administración de su servidor donde pueda acceder a los archivos.

- Paso 2: Navegar hasta el directorio de instalación de WordPress:
  Ir a wp-content>themes
  Buscar el archivo functions.php
- Paso 3: Abrir el archivo functions.php y copiar el siguiente código:

```
if (!is_admin()) {
// default URL format
if (preg_match('/author=([0-9]*)/i', $_SERVER['QUERY_STRING'])) die(); add_filter('redirect_canonical',
'shapeSpace_check_enum', 10, 2);
}
function shapeSpace_check_enum($redirect, $request) {
// permalink URL format
if (preg_match('/\?author=([0-9]*)(\/*)/i', $request)) die(); else return $redirect;
}
```

Método 2: Modificar el archivo .htaccess.

- Paso 1: Iniciar sesión en el servidor como administardor.
- Paso 2: En el administrador de archivos, busque el archivo .htaccess en la raíz de su servidor.
- Paso 3: Abrir el archivo .htaccess y copie el siguiente código:

```
<IfModule mod_rewrite.c>
RewriteCond %{QUERY_STRING} ^author=([0-9]*)
RewriteRule .* https://tusitioweb.com/? [L,R=302]
</IfModule>
```

3. Eliminar los mensajes de error en páginas de inicio de sesión

Para eliminar los mensajes de error detallados en la ventana de wp-login, debe ingresar el siguiente código en el archivo **functions.php** (Nota.- En caso de funcionar esta solución puede aplicar el código en el archivo **wp-login.php**):

```
<?php
//* NO incluyas la etiqueta de apertura


// Cambia el mensaje de error de inicio de sesión en WordPress


function failed_login() {
    return 'Las credenciales de acceso son incorrectas.';
```

```
}
add_filter('login_errors', 'failed_login');
```