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

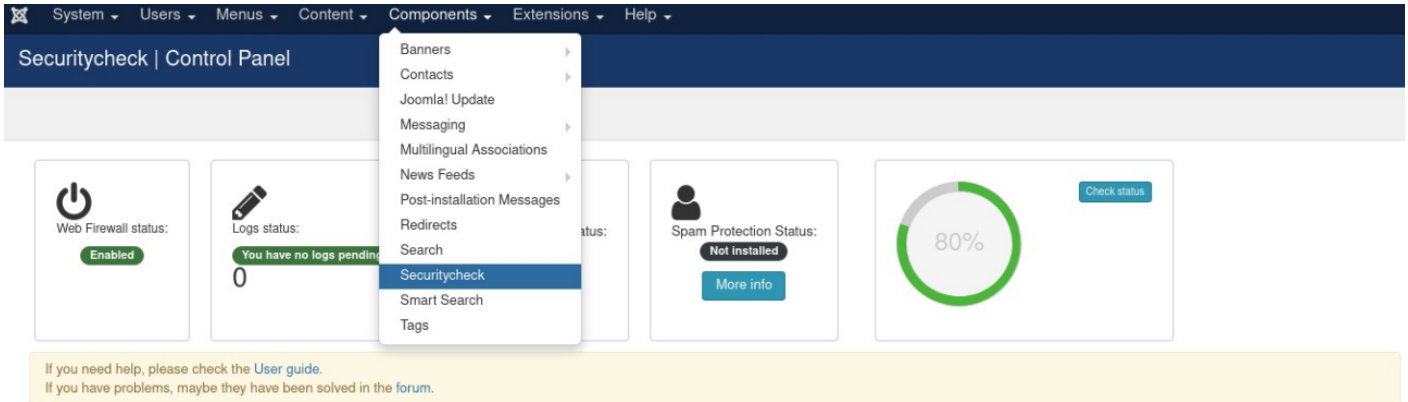
Comprobar regularmente si hay nuevos parches de seguridad disponibles para solucionar vulnerabilidades de seguridad e instalarlos, para ello existe el complemento “Plugin Securitycheck”.

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

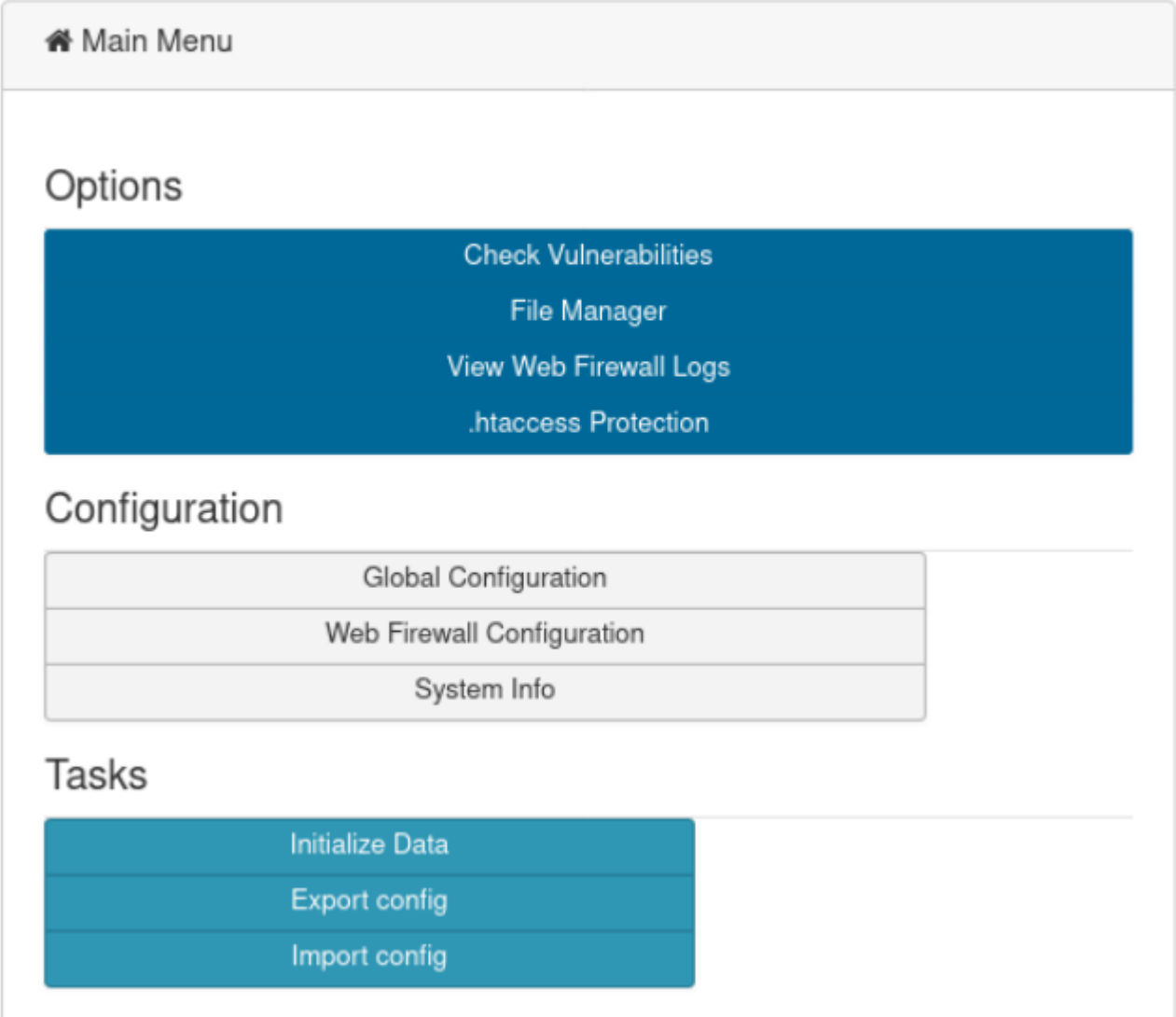
- Instalar el plugin siguiendo el enlace:

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

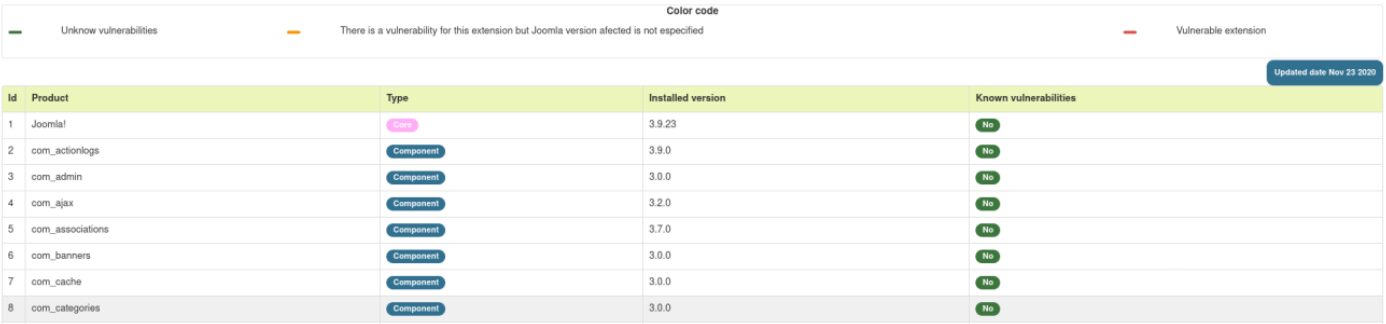
- Una vez instalado ir al menú Components→Securitycheck



- Verificar vulnerabilidades en los complementos.



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



Color code

Unknow vulnerabilities | There is a vulnerability for this extension but Joomla version afected is not especified | Vulnerable extension

Updated date Nov 23 2020

Id	Product	Type	Installed version	Known vulnerabilities
1	Joomla!	Core	3.9.23	No
2	com_actionlogs	Component	3.9.0	No
3	com_admin	Component	3.0.0	No
4	com_ajax	Component	3.2.0	No
5	com_associations	Component	3.7.0	No
6	com_banners	Component	3.0.0	No
7	com_cache	Component	3.0.0	No
8	com_categories	Component	3.0.0	No

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

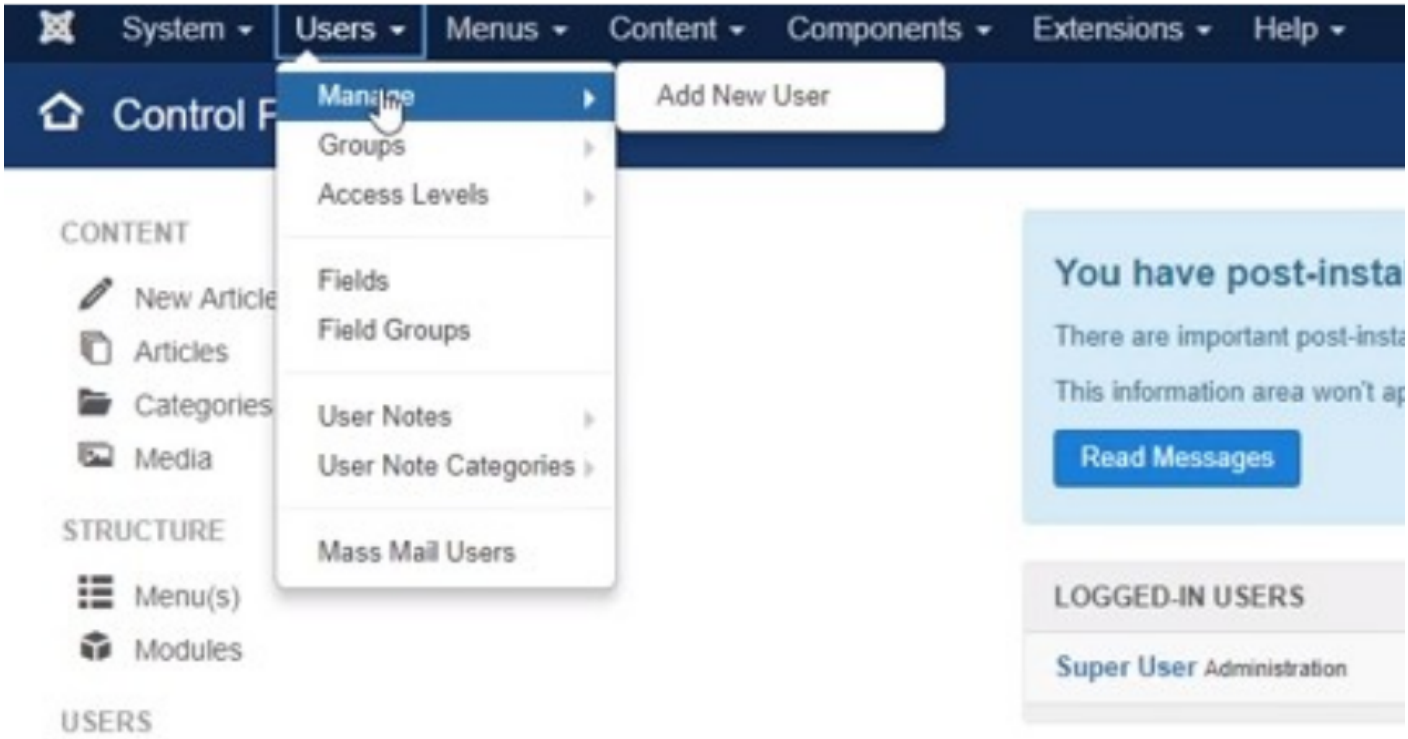
- https://docs.joomla.org/Security_hotfixes_for_Joomla_EOL_versions/es
- https://developer.joomla.org/security-centre.html

Siempre debe mantener actualizado Joomla a una versión con soporte.

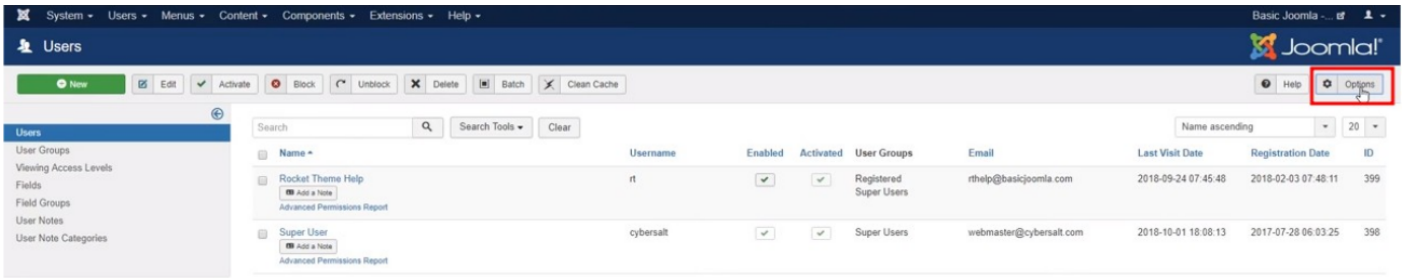
También se recomienda que se considere actualizar las tecnologías complementarias para el uso de Joomla como es php, mysql y el sistema operativo, tomando en cuenta que estas actualizaciones sean compatibles con la versión de Joomla que utiliza, aplicando estos cambios primero en un entorno de pruebas.

2.2. Asegurar nombre de usuario y contraseña

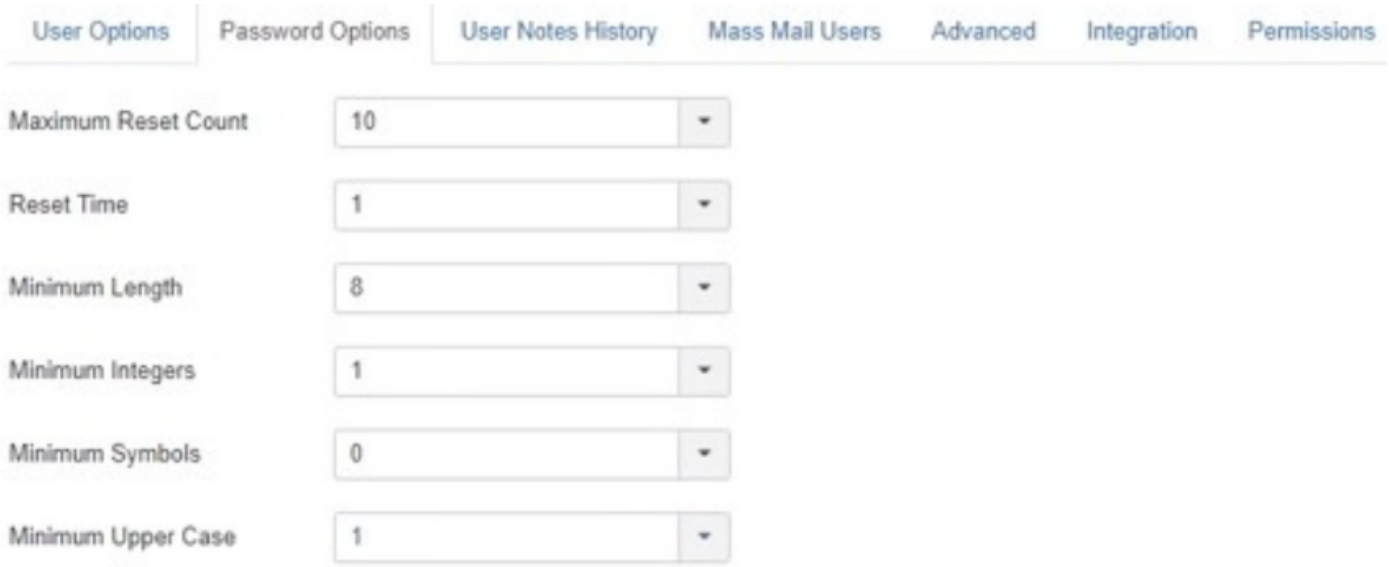
- No utilizar el nombre de usuario admin predeterminado.
- Utilizar una contraseña robusta, por ejemplo, que contenga mayúsculas, minúsculas, cifras y caracteres especiales.
- Configurar la robustez de la contraseña, para ello se debe ingresar a Users > Manage:



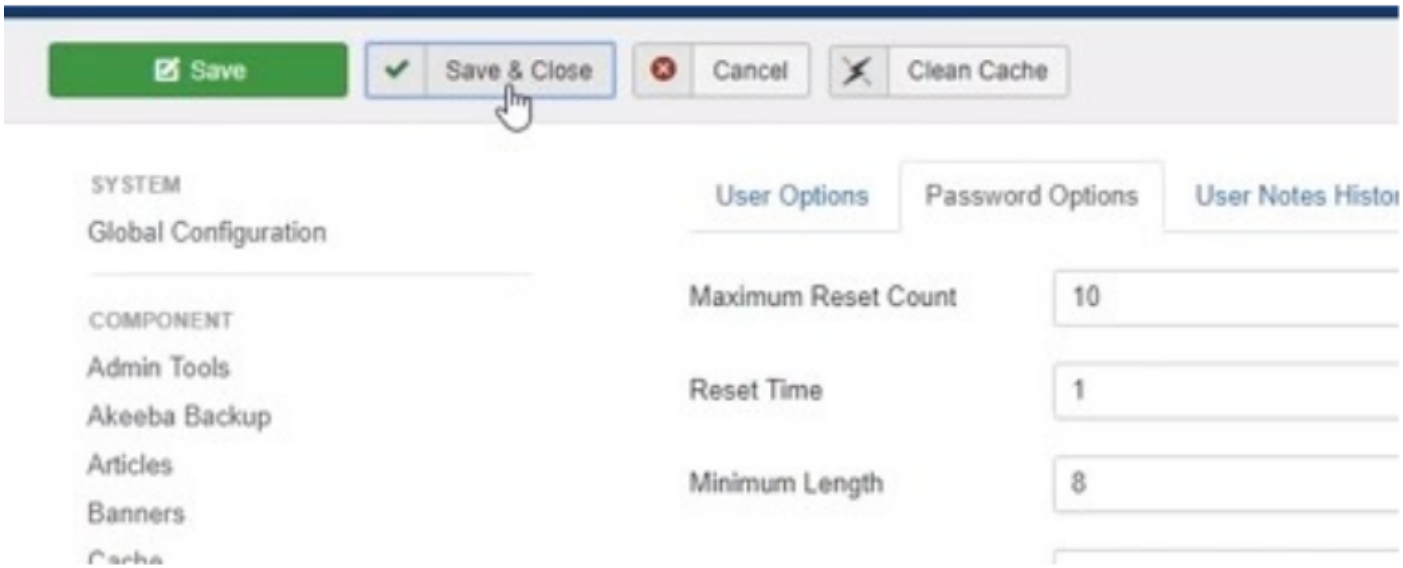
- Seleccionar Options:



- 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”.

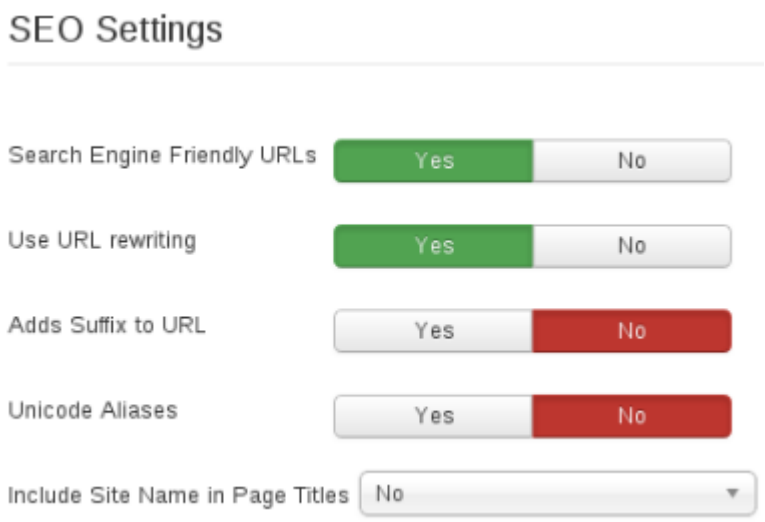
Adicionalmente, deberá eliminar la carpeta “installation” ubicada en el directorio raíz de la instalación de Joomla.

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”:



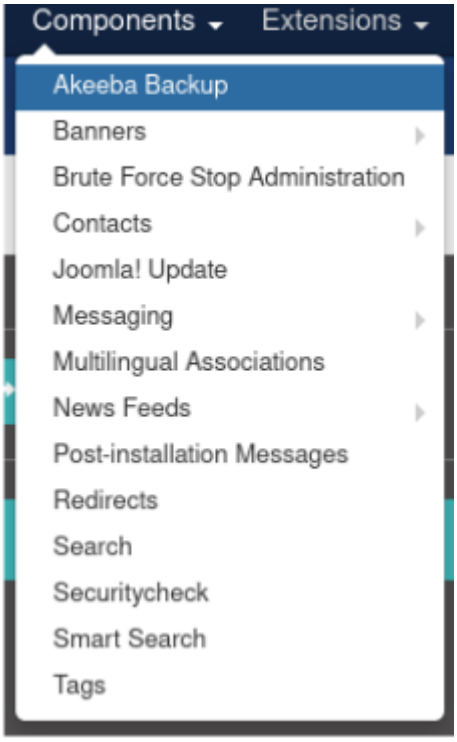
2.7. Realizar copia de seguridad

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

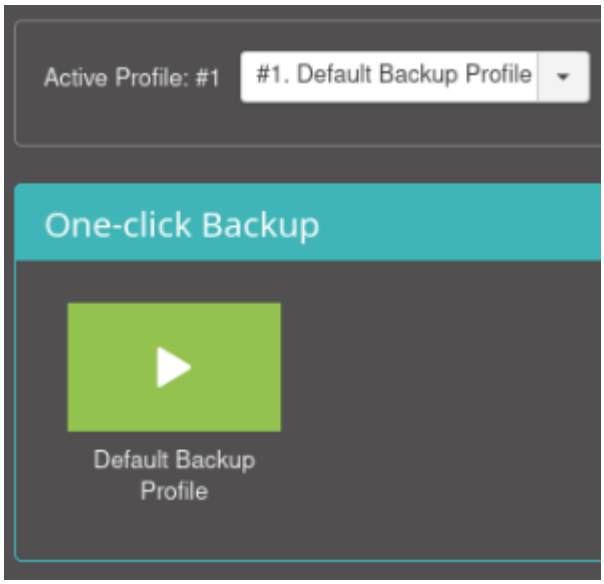
- Instalar el plugin siguiendo el enlace:

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

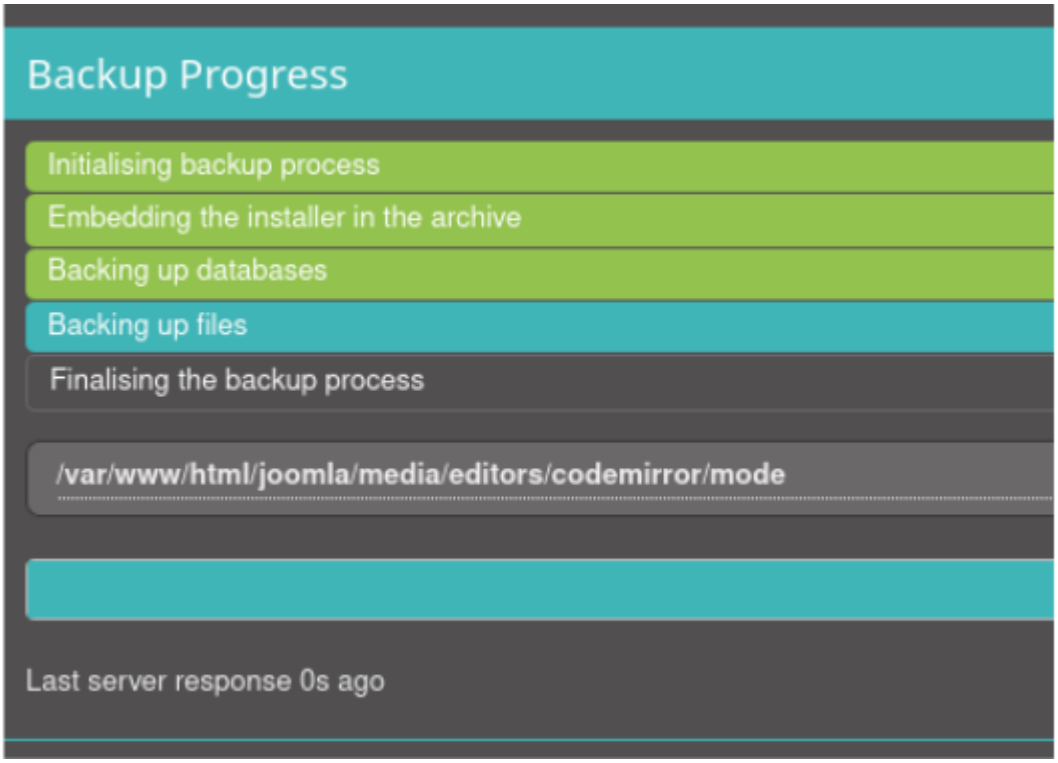
- Una vez instalado ir al menú Components>Akeeba Backup



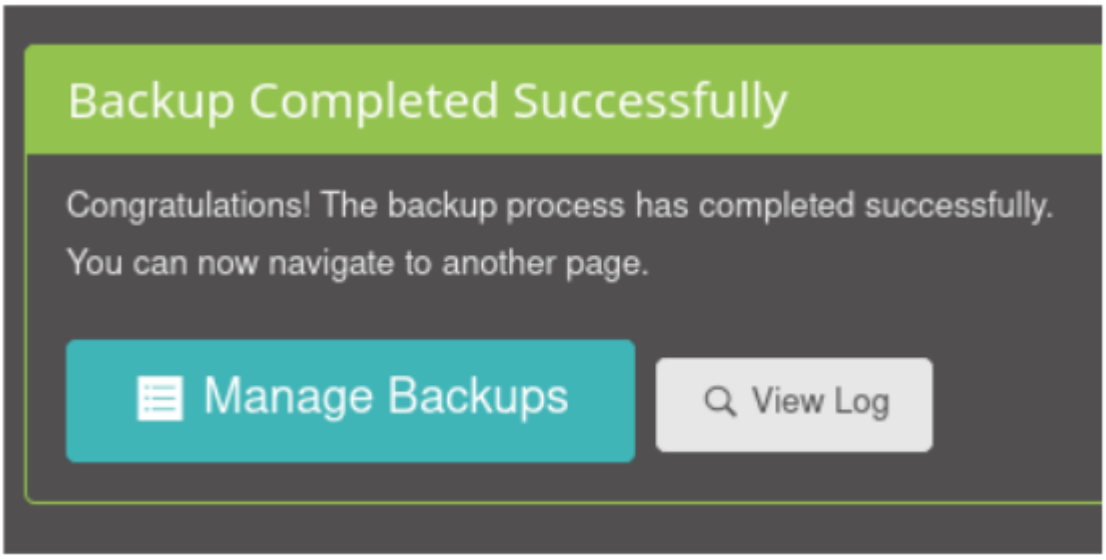
- Hacer clic en “Default Backup Profile” para sacar la copia de seguridad de Joomla.



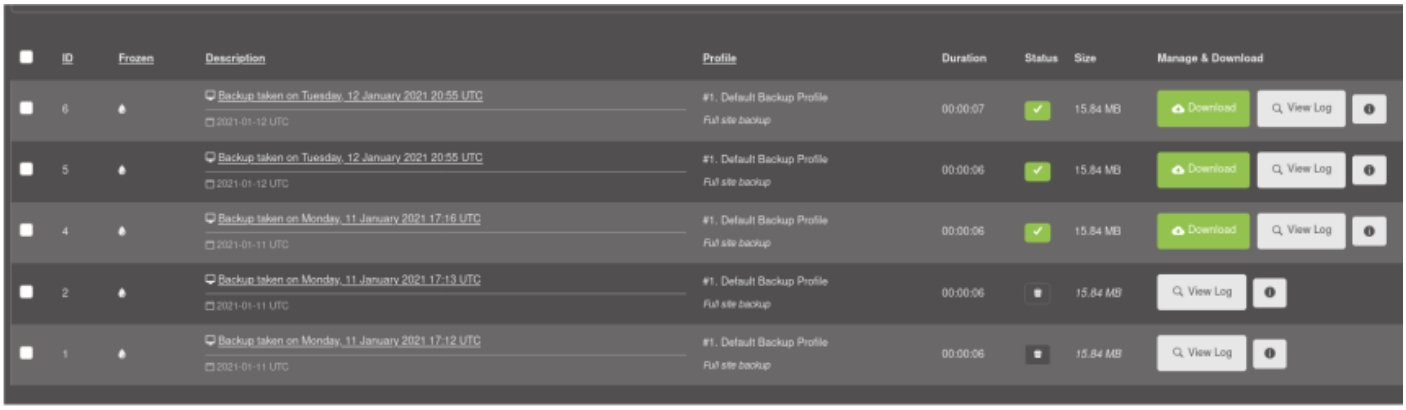
- Se despliega el proceso de backup



- Los backups se muestran en Manage Backups.



- Se muestra el listado de backups generados.



ID	Frozen	Description	Profile	Duration	Status	Size	Manage & Download
6		Backup taken on Tuesday, 12 January 2021 20:55 UTC 2021-01-12 UTC	#1. Default Backup Profile Full site backup	00:00:07	✓	15.84 MB	Download / View Log
5		Backup taken on Tuesday, 12 January 2021 20:55 UTC 2021-01-12 UTC	#1. Default Backup Profile Full site backup	00:00:06	✓	15.84 MB	Download / View Log
4		Backup taken on Monday, 11 January 2021 17:16 UTC 2021-01-11 UTC	#1. Default Backup Profile Full site backup	00:00:06	✓	15.84 MB	Download / View Log
2		Backup taken on Monday, 11 January 2021 17:13 UTC 2021-01-11 UTC	#1. Default Backup Profile Full site backup	00:00:06		15.84 MB	View Log
1		Backup taken on Monday, 11 January 2021 17:12 UTC 2021-01-11 UTC	#1. Default Backup Profile Full site backup	00:00:06		15.84 MB	View Log

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

Revision #4
Created 10 marzo 2023 10:59:52 by Franz Rojas
Updated 10 abril 2024 11:05:56 by Vladimir Urquiola