

Joomla comprometido

Revisiones Online

Verificar que no tenga instalado malware:

- <https://www.virustotal.com/#/home/upload>
- <https://sitecheck.sucuri.net/>
- <https://transparencyreport.google.com/safe-browsing/search>

Coordinación con el RSI

- Solicitar al RSI que no debe elimine ningun archivo ni realice cambios en la base de datos
- Si es un incidente de defacement, solicitar al RSI que establezca un sitio web temporal mientras dure la investigacion. En el archivo configuration.php configurar la variable \$offline = '1';
- Solicitar los archivos de la instalacion de jomla
- Solicitar el envio del backup de la base de datos
- Solicitar el envio de los logs del servidor web

Revisiones Offline

- Borrar themes no usados
- Borrar plugins no usados
- Revisar el archivo .htaccess, verificar que no hay redirecciones extrañas
- Verificar integridad de archivos core de la instalación de joomla con <https://audit-fs.co.za/>
- Descargar los componentes usados del repositorio oficial
- Actualizar el core: <https://www.youtube.com/watch?v=Duba0GEj2L8>
- Revisar integridad de archivos, comparar con los archivos descargados
<https://downloads.joomla.org/es/latest>

```
diff -r joomla-3.6.4 ./public_html
```

Restauración del sitio

- Eliminar los backdoors identificados y restaurar el sitio web con los archivos antiguos

- Cambiar las contraseñas de los usuarios de:
 - Joomla
 - Base de datos
 - hosting/Cpanel

Modificar permisos:

- `chmod 444 .htaccess`
- `chmod 444 index.php`

Instalar las extensiones

- <https://extensions.joomla.org/extension/securitycheck/> (Revisa componentes con vulnerabilidades)
- <https://www.akeebabackup.com/products/akeeba-backup.html> (Realizar backups)
- <https://extensions.joomla.org/extension/brute-force-stop/>
- <https://www.richeyweb.com/software/joomla/plugins/1-adminexile/>

Reemplazar el contenido del archivo `.htaccess` con:

Herramientas

<https://malwaredecoder.com>

Actualización del core de Joomla a la última versión

1. Descargar el paquete de actualización <https://downloadas.joomla.org/es/>
2. Sobre escribir los archivos en el servidor con los del paquete de actualización.
3. Si sale el error "Fatal error: Call to undefined method JApplicationSite::set()"
 1. Reemplazar la carpeta `libraries` con las de la instalación completa.
4. Si sale un error "Unknown column 'a.cliente_id' in 'where clause': Unknown column 'a.client_id' in 'where clause'" en el panel de administración.
 1. Ejecutar (Reemplazar XXXXX por el prefijo usado en la base de datos):

```
ALTER TABLE `XXXXXX_menu_types` ADD COLUMN `client_id` int(11) NOT NULL DEFAULT 0 AFTER `description`;
```

```
UPDATE `XXXXXX_menu` SET `published` = 1 WHERE `menutype` = 'main' OR `menutype` = 'menu';
```

Realizar correcciones en la base de datos. En el menú de administración:

Extensiones> Gestor de extensiones> Database> Corregir

Hardening de Joomla

- Cambiar el nombre del usuario administrador (admin) y crear un password robusto
- Los archivos deben tener los siguientes permisos:

Tipo de archivo	Permisos
Archivos PHP	644
Archivos de configuración	644
Otros folders	755

- Cambiar la ruta por defecto del panel de administración
- Deshabilitar el registro de usuarios:

tudominio.com/administrador/index.php?option=com_config&view=component&component=com_users

Revision #5

Created 6 marzo 2023 18:14:11 by Vladimir Urquiola

Updated 10 marzo 2023 10:58:45 by Franz Rojas