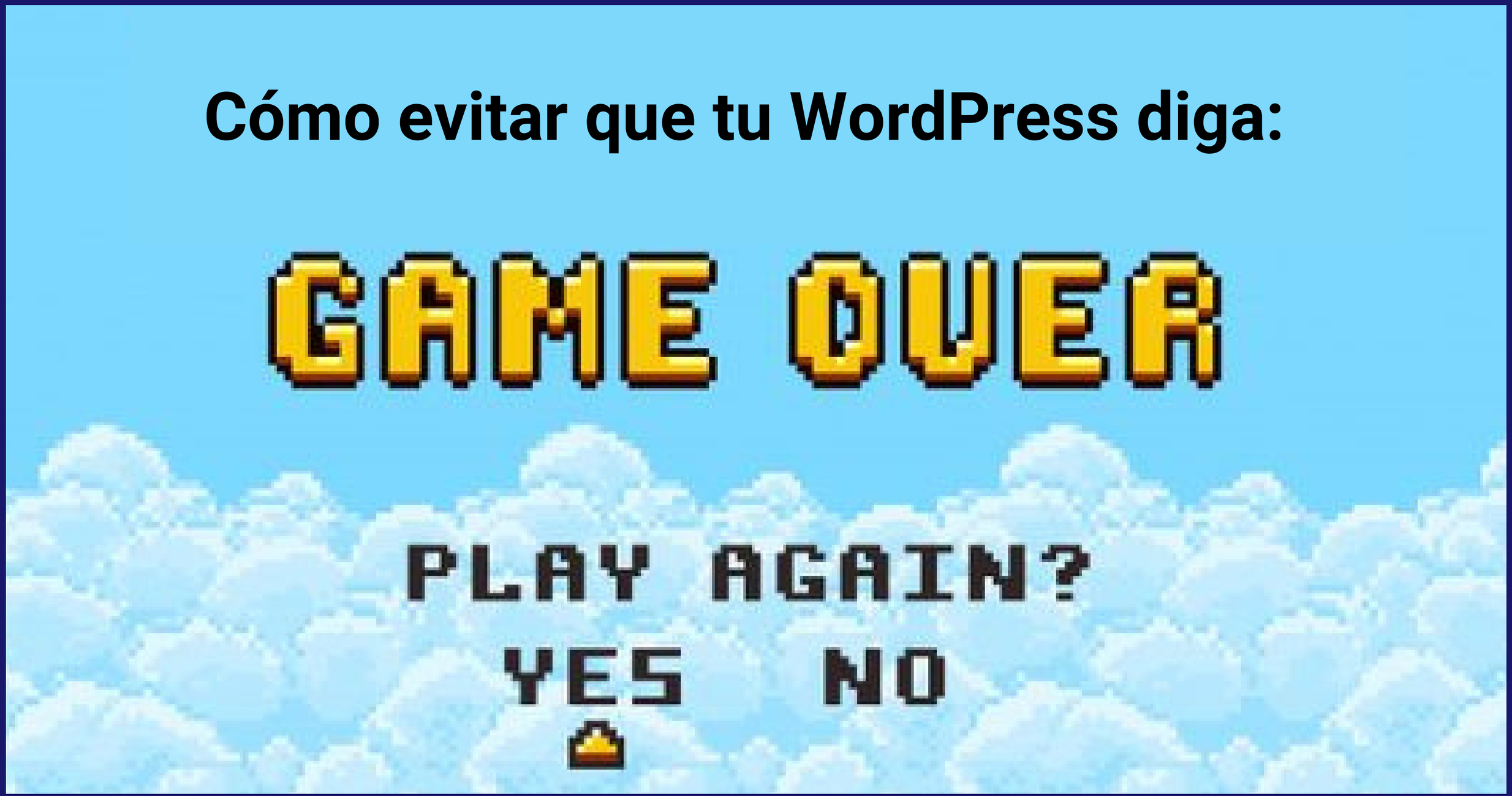
ÉRICA AGUADO

Administradora de Sistemas especializada en ciberseguridad para plataformas online.

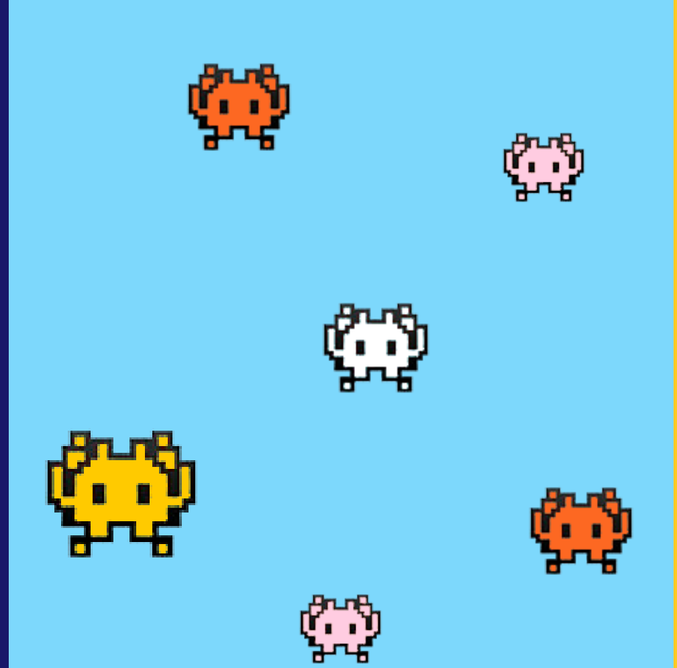
De día crio un bicho,
de noche cazo ciberbichos.

Cómo evitar que tu WordPress diga:



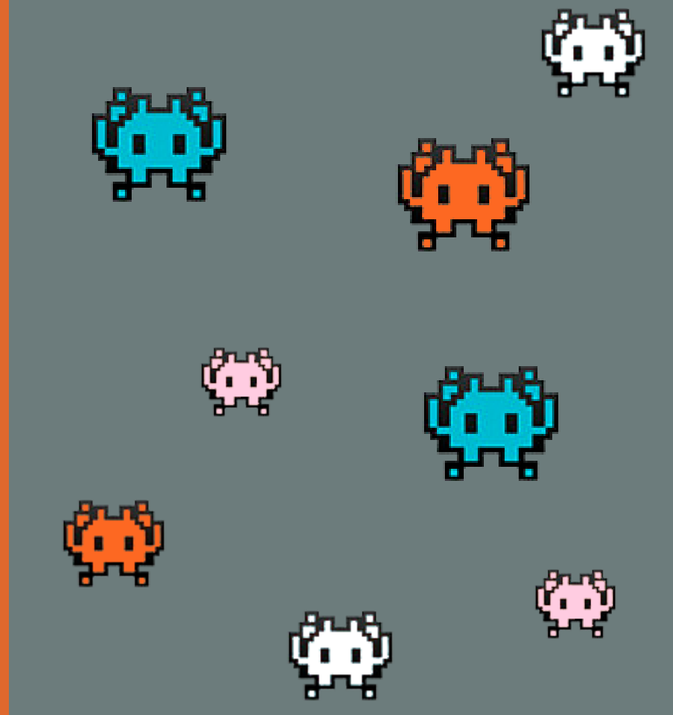
Por qué atacan a los sitios web con WP?

Respuesta "de cajón"...



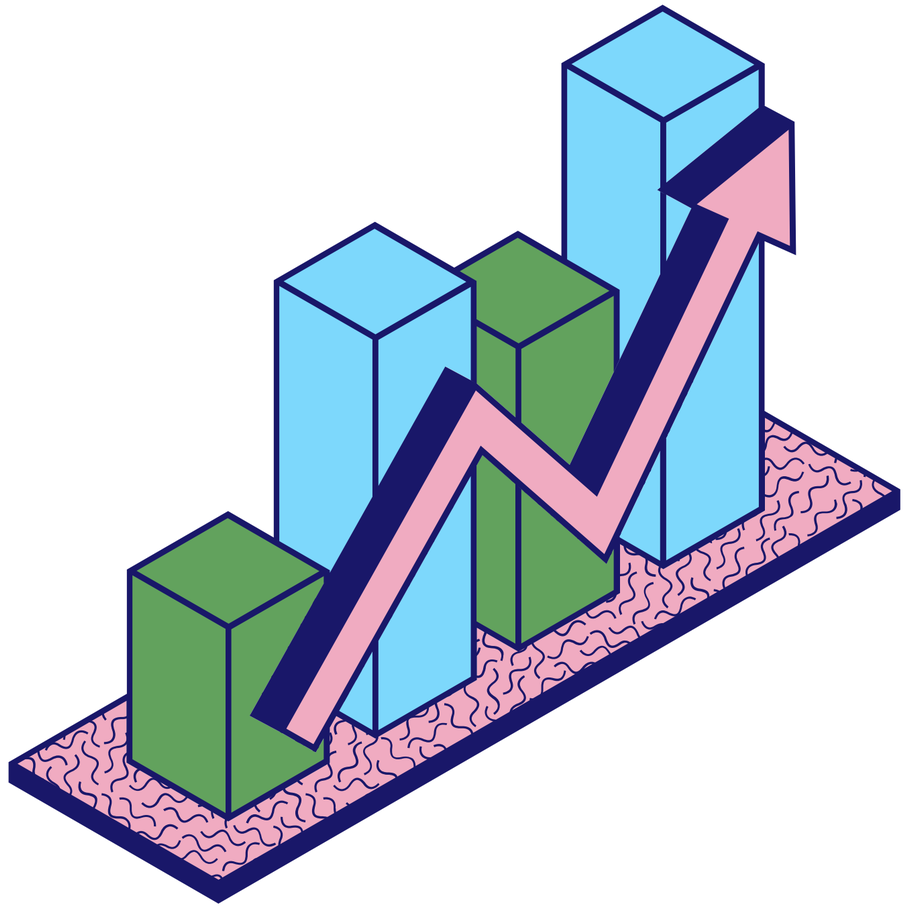
Más webs

Más ataques



Las campañas maliciosas funcionan por estadísticas.

Sus autores saben que existe un cierto porcentaje de usuarios, aunque sea pequeño, que caerá en su trampa.



Twitter de @erica_aguado

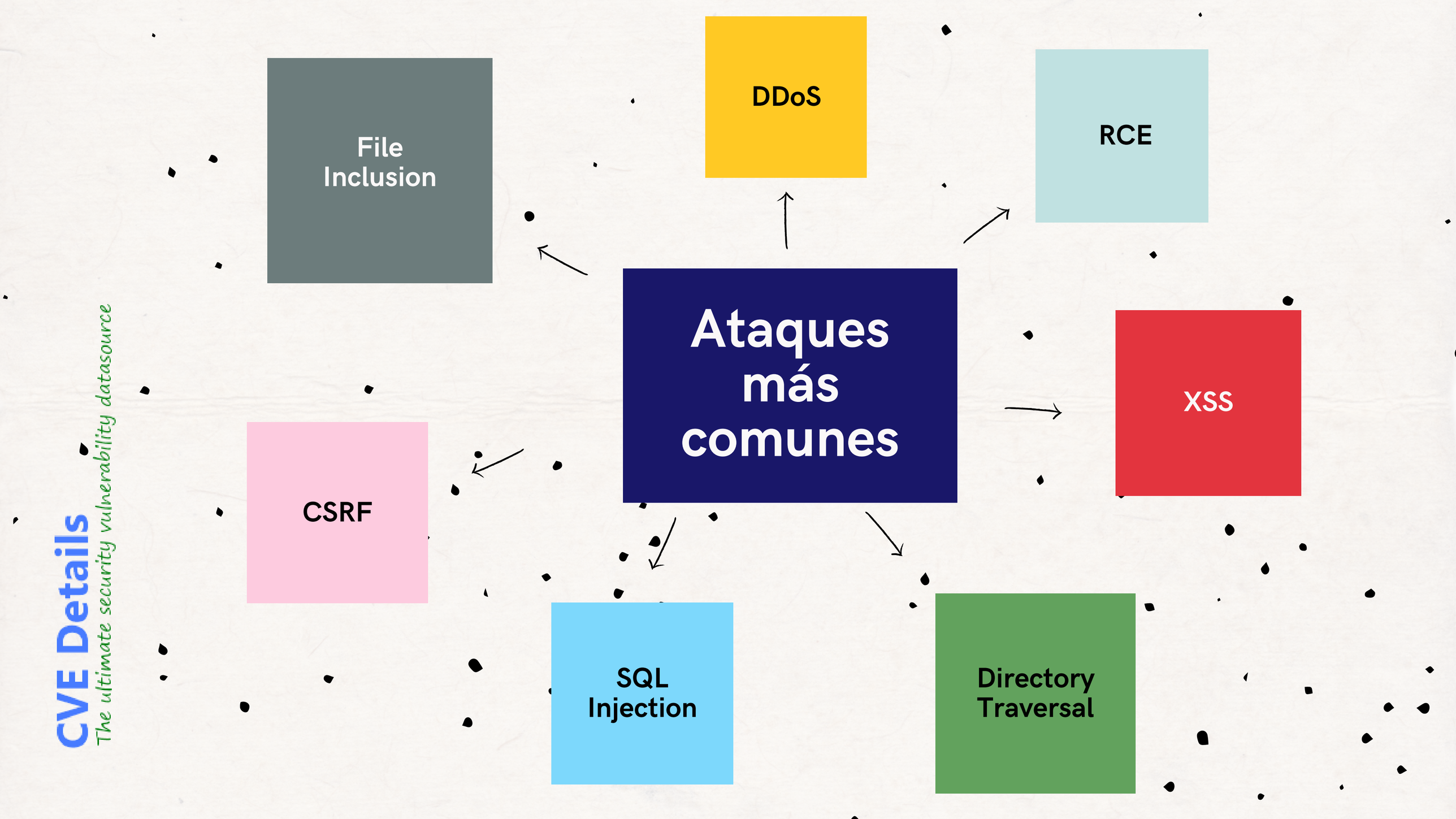
Qué es eso de la SEGURIDAD

Que se nos olvida...

El propósito de la SEGURIDAD WEB es prevenir de posibles ataques

La seguridad de sitios web requiere de esfuerzos en todo el ecosistema web:

1- En la aplicación web (WordPress, Prestashop, etc...)
2. En la configuración del servidor web
3. En las políticas de administración de usuarios
4. En el código del lado cliente (Navegador, etc...)


File Inclusion
DDoS
RCE
Ataques más comunes
XSS
CSRF
SQL Injection
Directory Traversal
CVE Details
The ultimate security vulnerability datasource

DDoS

Distributed Denial of Service (denegación de servicio distribuido).

Es un ataque que se lleva a cabo generando un gran flujo de información desde varios puntos de conexión hacia un mismo punto de destino, provocando la pérdida de conectividad por el elevado consumo de ancho de banda o por la sobrecarga de recursos.

La forma más común de realizar un DDoS es a través de una red de bots (botnet).

Cómo evitarlo

- **Desactivar API Rest y XML-RCP**
- **Limitar intentos de acceso**
- **Desactivar pingbacks y trackbacks**
- **Firewall y WAF**
- **Activar protección antibots**
- **Desactivar concatenación de scripts**

Ejemplos DDoS

incibe-cert_

Alerta ▾ Incidentes ▾ Servicios Publicaciones ▾ Sobre INCIBE-CERT ▾

Inicio / Alerta Temprana / Vulnerabilidades / CVE-2018-6389

Vulnerabilidad en WordPress (CVE-2018-6389)

Tipo: Consumo de recursos no controlado (Agotamiento de recursos)
Gravedad: Media
Fecha publicación : 06/02/2018
Última modificación: 01/03/2019

Descripción

En WordPress hasta la versión 4.9.2, los atacantes no autenticados puede provocar una denegación de servicio (consumo de recursos) utilizando una lista grande de archivos .js registrados (de wp-includes/script-loader.php) para construir una serie de peticiones para cargar cada archivo muchas veces.

Impacto

Vector de acceso: A través de red

Complejidad de Acceso: Baja

Autenticación: No requerida para explotarla

Tipo de impacto: No hay impacto en la integridad del sistema + No hay impacto en la confidencialidad del sistema + Afecta parcialmente a la disponibilidad del sistema




CIBERSEGURIDAD

Una oleada de ciberataques en Andorra afecta a algunos de los streamers españoles más populares

• Andorra Telecom ha informado esta mañana del tercer ataque de DDos en tres días: hubo otros dos el viernes y el sábado

RCE

Remote Code Execution

La ejecución de código remoto se trata de una vulnerabilidad que permite cargar y ejecutar código o comandos remotamente aprovechando un fallo en la programación o alguna función de PHP.

Cómo evitarlo

- **Actualizaciones al día**
- **Cambiar prefijo base de datos**
- **Utilizar la última versión de PHP.**
- **Prohibir PHP en el directorio wp-includes, uploads y cache.**
- **Desactivar lenguajes de scripting no usados (Python, perl, etc...)**
- **Validar las peticiones de entrada de usuarios (plugins)**

Ejemplo RCE

incibe-cert_ Alerta Incidentes Servicios Publicaciones Sobre INCIBE-CERT

Inicio / Alerta Temprana / Vulnerabilidades / CVE-2021-24209

Vulnerabilidad en una página de configuración en la opción WP Super Cache Settings-) Cache Location en el plugin WordPress WP Super Cache (CVE-2021-24209)

Tipo: Validación incorrecta de entrada
Gravedad: Alta
Fecha publicación : 05/04/2021
Última modificación: 04/05/2021

Descripción

El plugin WordPress WP Super Cache versiones anteriores a 1.7.2, estuvo afectado por una RCE autenticado (admin+) en la página de configuración debido a una falta de comprobación de entrada y una comprobación débil de $cache_path en la opción WP Super Cache Settings-) Cache Location. El acceso directo al archivo wp-cache-config.php no está prohibido, por lo que esta vulnerabilidad puede ser explotada para una inyección de shell web

Impacto

Vector de acceso: A través de red

Complejidad de Acceso: Baja

Autenticación: No disponible

Tipo de impacto: Compromiso total de la integridad del sistema + Compromiso total de la confidencialidad del sistema + Compromiso total de la disponibilidad del sistema

Productos y versiones vulnerables

- cpe:2.3:a:automattic:wp_super_cache:*:*:*:*:*:wordpress:*:*

Para consultar la lista completa de productos y versiones ver esta página

Referencias a soluciones, herramientas e información

- https://plugins.trac.wordpress.org/changeset/2496238/wp-super-cache (Origen: MISC)
- https://m0ze.ru/vulnerability/[2021-03-13]-[WordPress]-[CWE-94]-WP-Super-Cache-WordPress-Plugin-v1.7.1.txt (Origen: MISC)
- https://wpscan.com/vulnerability/733d8a02-0d44-4b78-bbb2-37e447acd2f3 (Origen: CONFIRM)

Explicación de los campos

Ir atrás





XSS

Los ataques XSS también llamados en inglés Cross-site scripting son un tipo de ataque que aprovecha vulnerabilidades en el código que permitirían a una tercera persona inyectar, en páginas web visitadas por el usuario, código JavaScript no autorizado y ejecutarlo.

El script malicioso se podría ejecutar almacenándolo en el servidor o directamente en el lado del usuario en el navegador.

Cómo evitarlo

- Cookies de sesión con HTTPOnly y Secure Flag
- Desactivar/limitar cabecera HTTP X-Frame-Options
- Encabezado HTTP seguros, como Content Security Policy (CSP)
- Desactivar el HTTP TRACE / TRACK
- Firewall

Ejemplo XSS

incibe-cert_

Alerta | Incidentes | Servicios | Publicaciones | Sobre INCIBE-CERT

Inicio / Alerta Temprana / Vulnerabilidades / CVE-2021-24381

Vulnerabilidad en el nombre de la clase personalizada del campo form en el plugin Ninja Forms Contact Form de WordPress (CVE-2021-24381)

Tipo: Neutralización incorrecta de la entrada durante la generación de la página web (Cross-site Scripting)
Gravedad: Baja
Fecha publicación : 25/10/2021
Última modificación: 28/10/2021

Descripción

El plugin Ninja Forms Contact Form de WordPress versiones anteriores a 3.5.8.2, no sanea ni escapa del nombre de la clase personalizada del campo form creado, lo que podría permitir a usuarios con altos privilegios llevar a cabo ataques de tipo Cross-Site Scripting incluso cuando la capacidad unfiltered_html está deshabilitada

Impacto

Vector de acceso: A través de red

Complejidad de Acceso: Media

Autenticación: No disponible

Tipo de impacto: Afecta parcialmente a la integridad del sistema + No hay impacto en la confidencialidad del sistema + No hay impacto en la disponibilidad del sistema

Productos y versiones vulnerables

- cpe:2.3:a:ninjaforms:contact_form:*:*:*:*:*:*:wordpress:*:*

Para consultar la lista completa de productos y versiones ver esta página

Referencias a soluciones, herramientas e información

- https://wpscan.com/vulnerability/e383fae6-e0da-4aba-bb62-adf51c01bf8d (Origen: MISC)

Explicación de los campos

Ir atrás





Directory Traversal

Los ataques por cruce de directorios son un ataque HTTP que permite a un atacante aprovechar una vulnerabilidad en el recorrido de directorios para listar directorios o acceder a archivos.

Cómo evitarlo

- Bloquear exploración de directorios
- Permisos de ficheros
- Bloquear el acceso a archivos confidenciales
- Bloquear análisis author
- Ocultar versiones
- Firewall o Waf
- Evitar plugins de subida o modificación de ficheros.

Ejemplo DIRECTORY TRAVERSAL

incibe-cert_ Alerta Incidentes Servicios Publicaciones Sobre INCIBE-CERT

Inicio / Alerta Temprana / Vulnerabilidades / CVE-2021-34638

Vulnerabilidad en los archivos de configuración en WordPress Download Manager (CVE-2021-34638)

Tipo: Limitación incorrecta de nombre de ruta a un directorio restringido (Path Traversal)
Gravedad: Media
Fecha publicación : 05/08/2021
Última modificación: 12/08/2021

Descripción

Un Salto de Directorio Autenticado en WordPress Download Manager versiones anteriores a 3.1.24 incluyéndola, permite a usuarios autenticados (Contributor+) obtener información confidencial de archivos de configuración, además de permitir a usuarios Author+ llevar a cabo ataques de tipo XSS, al ajustar Download template a un archivo que contiene información de configuración o un JavaScript cargado con una extensión de imagen Este problema afecta a: WordPress Download Manager versión 3.1.24 y versiones anteriores

Impacto

Vector de acceso: A través de red

Complejidad de Acceso: Baja

Autenticación: No disponible

Tipo de impacto: No hay impacto en la integridad del sistema + Afecta parcialmente a la confidencialidad del sistema + No hay impacto en la disponibilidad del sistema

Productos y versiones vulnerables

- cpe:2.3:a:wpdownloadmanager:wordpress_download_manager:*:*:*:*:*:wordpress:*:*

Para consultar la lista completa de productos y versiones ver esta página

Referencias a soluciones, herramientas e información

- https://www.wordfence.com/blog/2021/07/wordpress-download-manager-vulnerabilities/ (Origen: MISC)

Explicación de los campos

Ir atrás





SQL Injection

Los ataques por Inyección SQL aprovechan vulnerabilidades para infiltrar o incrustar código SQL intruso aprovechando la falta de comprobación de las variables con el fin de quebrantar las medidas de seguridad y acceder a datos protegidos.

Cómo evitarlo

- Actualizaciones
- Configuración de las Security Keys
- Cambia el prefijo de la base de datos
- Evita la inyección de scripts
- Proteger htaccess y wp-config.php
- Prevenir el indice de directorios en robots.txt
- Sanitizar el contenido de variables.

Ejemplo SQL INJECTION

incibe-cert_

Alerta ▾ Incidentes ▾ Servicios Publicaciones ▾ Sobre INCIBE-CERT ▾

Inicio / Alerta Temprana / Vulnerabilidades / CVE-2021-24726

Vulnerabilidad en el parámetro orderby en la acción Search Calendars en el plugin WP Simple Booking Calendar de WordPress (CVE-2021-24726)

Tipo: Neutralización incorrecta de elementos especiales usados en un comando SQL (Inyección SQL)
Gravedad: Media
Fecha publicación : 13/09/2021
Última modificación: 23/09/2021

Descripción

El plugin WP Simple Booking Calendar de WordPress versiones anteriores a 2.0.6, no escapaba, comprobaba o saneaba el parámetro orderby en su acción Search Calendars, antes de usarlo en una sentencia SQL, conllevando a un problema de inyección SQL autenticada

Impacto

Vector de acceso: A través de red

Complejidad de Acceso: Baja

Autenticación: No disponible

Tipo de impacto: Afecta parcialmente a la integridad del sistema + Afecta parcialmente a la confidencialidad del sistema + Afecta parcialmente a la disponibilidad del sistema

Productos y versiones vulnerables

- cpe:2.3:a:wpsimplebookingcalendar:wp_simple_booking_calendar:*:*:*:*:*:wordpress:*:*

Para consultar la lista completa de productos y versiones ver esta página

Referencias a soluciones, herramientas e información

- https://wpscan.com/vulnerability/f85b6033-d7c1-45b7-b3b0-8967f7373bb8 (Origen: MISC)
- https://www.trustwave.com/en-us/resources/security-resources/security-advisories/?fid=29176 (Origen: MISC)

Explicación de los campos

< Ir atrás





CSRF

Cross-site request forgery o falsificación de petición en sitios cruzados.

Fuerza al navegador web de un usuario registrado a enviar una petición que pasa por otra aplicación, y la utiliza para realizar una acción maliciosa en nombre del usuario.

Se suele usar para estafas por Internet y el proceso se lleva a cabo mediante solicitudes HTTP.

Cómo evitarlo

- **HTTPS (HSTS)**
- **Usar última versión de PHP**
- **Configuración cabeceras HTTP seguras**
- **Impedir acceso a servidores externos**
- **Evitar subida de ficheros en formularios**
- **Firewall**
- **Control de ficheros y código**

Ejemplo CSRF

incibe-cert_

Alerta | Incidentes | Servicios | Publicaciones | Sobre INCIBE-CERT

Inicio / Alerta Temprana / Vulnerabilidades / CVE-2022-0328

Vulnerabilidad en el plugin Simple Membership de WordPress (CVE-2022-0328)

Tipo: Falsificación de petición en sitios cruzados (Cross-Site Request Forgery)
Gravedad: Sin asignar
Fecha publicación : 28/02/2022
Última modificación: 28/02/2022

Descripción

El plugin Simple Membership de WordPress versiones anteriores a 4.0.9, no presenta comprobación de tipo CSRF cuando son eliminados miembros en masa, lo que podría permitir a atacantes hacer que un administrador conectado los elimine por medio de un ataque de tipo CSRF

Impacto

Vector de acceso: No disponible

Complejidad de Acceso: No disponible

Autenticación: No disponible

Tipo de impacto: No disponible

Referencias a soluciones, herramientas e información

- https://wpscan.com/vulnerability/44532b7c-4d0d-4959-ada4-733f377d6ec9 (Origen: MISC)
- https://plugins.trac.wordpress.org/changeset/2662855 (Origen: CONFIRM)

Explicación de los campos

Ir atrás





File Inclusion

Ataque por FI (del inglés File Inclusion, traducido al español como Inclusión de Archivos)

Es un tipo de ataque que aprovecha alguna vulnerabilidad en una página web que permite al usuario leer, modificar y/o subir archivos al servidor.

Cómo evitarlo

- **Actualizaciones**
- **Permisos de ficheros**
- **Utilizar últimas versiones de PHP**
- **Prohibir PHP en los directorios wp-includes, uploads y cache.**
- **Evitar usar plugins de subida de ficheros.**
- **Deshabilitar la edición de ficheros.**
- **Firewall o WAF**

Ejemplo File Inclusion

incibe-cert_ Alerta Incidentes Servicios Publicaciones Sobre INCIBE-CERT

Inicio / Alerta Temprana / Vulnerabilidades / CVE-2021-24970

Vulnerabilidad en el parámetro tab en el plugin All-in-One Video Gallery de WordPress (CVE-2021-24970)

Tipo: Limitación incorrecta de nombre de ruta a un directorio restringido (Path Traversal)
Gravedad: Media
Fecha publicación : 13/12/2021
Última modificación: 16/12/2021

Descripción

El plugin All-in-One Video Gallery de WordPress versiones anteriores a 2.5.0, no sanea ni comprueba el parámetro tab antes de usarlo en una sentencia requiere en el panel de administración, conllevando a un problema de inclusión de archivos locales

Impacto

Vector de acceso: A través de red

Complejidad de Acceso: Baja

Autenticación: No disponible

Tipo de impacto: Afecta parcialmente a la integridad del sistema + Afecta parcialmente a la confidencialidad del sistema + Afecta parcialmente a la disponibilidad del sistema

Productos y versiones vulnerables

- cpe:2.3:a:plugins360:all-in-one_video_gallery:*:*:*:*:*:wordpress:*:*

Para consultar la lista completa de productos y versiones ver esta página

Referencias a soluciones, herramientas e información

- https://wpscan.com/vulnerability/9b15d47e-43b6-49a8-b2c3-b99c92101e10 (Origen: MISC)

Explicación de los campos

Ir atrás

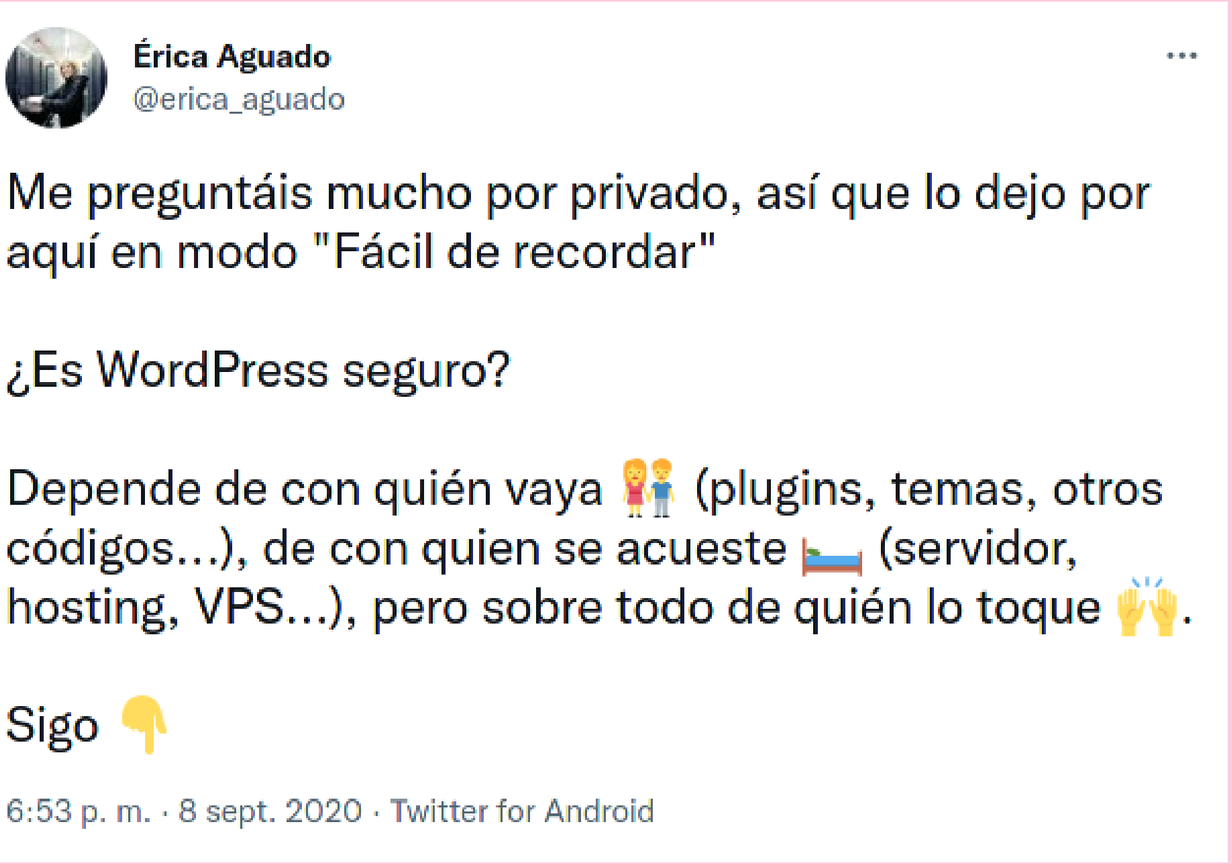




¿Es WordPress seguro?

La gran pregunta...

Si solo dependiera de WordPress...



Muchas gracias!

erica_aguado

erica-aguado-exposito

@erica_aguado

info@ericaaguado.es

MeetUp WordPress Valencia