4.2.3. All In One WP Security

Permite habilitar numerosas medidas de seguridad (algunas ya están en Wordfence) para nuestro Wordpress. Este plugin indica el grado de protección que tenemos con un interesante gráfico en forma de cuentakilómetros.

> Se configura en: Menú > Seguridad WP

Cambiar la dirección de acceso al Escritorio de Wordpress

La opción más interesante a configurar consiste en **cambiar la dirección de acceso al Escritorio de Wordpress**, de forma que ya no sea http://nombredelwordpress.es/wp-admin/, sino que escojamos una dirección diferente a **wp-admin**, para evitar que los hacker maliciosos intenten acceder a nuestro Wordpress entrando por la dirección por defecto wp-admin que es conocida por todo el mundo. Una vez cambiada la dirección de acceso, desconocerán cual es la dirección de acceso al Escritorio y se reducirá la cantidad de intentos de acceso fraudulentos. Si procedes a cambiar la dirección de acceso al Escritorio, será muy importante que apuntes tu nueva dirección de acceso al Escritorio de tu Wordpress, sino correrás el riesgo de quedarte sin acceso a administrar tu propio Wordpress.

> Se configura en: Menú > Seguridad WP > Fuerza Bruta > Cambiar el nombre de la página de entrada
> Login Page URL (por ejemplo): mizonadegestion

Ahí conviene que cada administrador de Wordpress escoja el nombre que desee, incluso con un nombre diferente a "mizonadegestion", para que no sea tan genérico. De esta forma, la nueva dirección de acceso al Escritorio será similar a:

http://nombredelwordpress.es/mizonadegestion/

Otras opciones a revisar de este plugin:

- Opciones > WP Version Info: Eliminar generador WP Meta Info: SI
- Cuentas de usuario > Mostrar nombre: Revisa que los Nombres de usuario estén ocultos y se muestre el alias
- Ingreso de usuarios > Activar característica de bloqueo de inicio de sesión: SI
- Ingreso de usuarios > Cerrar inicio de sesión: múltiples opciones

- Ingreso de usuarios > Forzar salir > Habilitar el cierre de sesión de usuario de Fuerza WP: si
- Ingreso de usuarios > Mostrar mensaje de error genérico: SI
- Seguridad del sistema de archivos: Deshabilitar "Edición archivo PHP".
- Seguridad del sistema de archivos > WP acceso archivo > Impedir el Acceso a Archivos de Instalación Predeterminada de WP: si
- Cortafuegos > Reglas basicas de Cortafuegos > Habilitar proteccion basica de Firewall: SI
- Cortafuegos > Reglas basicas de Cortafuegos > Bloquear el Acceso al Archivo debug.log : SI
- Cortafuegos > Reglas basicas de Cortafuegos > Bots de Internet > Bloquear falsos Googlebots: SI
- Cortafuegos > Prevenir enlaces activos > Evitar Hotlinking de Una Imagen: SI
- **Fuerza Bruta > Login Captcha > Habilitar Capcha en pagina de ingreso: SI** (*)
- **Fuerza Bruta > Login Captcha > Habilitar Captcha en Página de recuperar contraseña: SI** (*)
- Fuerza Bruta > Honeypot > Habilitar Honeypot En La Página De Entrada : SI
- Escáner: detección de cambios en los archivos, porque si hay cambios no deseados es probable que sean hackeos.

(*) Las opciones de habilitar **Captcha** proporcionan un gran incremento en la seguridad del Wordpress, ya que evitan que se realicen ataques automatizados intentando adivinar las contraseñas los usuarios del Wordpress.

Revision #6
Created 25 April 2022 08:30:04 by Equipo CATEDU
Updated 29 June 2022 13:28:16