

4.2.2. Wordfence

El plugin Wordfence tiene dos pilares básicos:

- Escanear el Wordpress en busca de hackeos
- Activar características para proteger el Wordpress (llamado firewall). Es interesante la opción de limitar el tráfico, ya que evitará que se realicen ataques de fuerza bruta contra tu Wordpress.

ESCANEAR EL WORDPRESS

1º **Wordfence** compara lo que tenemos en nuestro servidor con los repositorios oficiales. **Por ello, primero requiere que tengamos todo actualizado.**

2º Hay que configurar las opciones de escaneo en `Wordfence Scan Options > Options` Hay que activar casi todas las opciones para un escaneo más profundo, revisando estas opciones:

- Scan theme files against repository versions for changes: Activar
- Scan plugin files against repository versions for changes: Activar
- Scan files outside your WordPress installation: Probar a activarlo porque realiza una búsqueda más profunda, pero si se activa, puede que el escaneo tarde muchísimo o que no termine nunca porque entre en un bucle.
- Scan images, binary, and other files as if they were executable: Ralentiza mucho pero puede llegar a ser útil en algún ataque muy concreto.
- Enable HIGH SENSITIVITY scanning (may give false positives): Habilita un escaneo muy sensible, si se activa puede que dé muchos falsos positivos.
- Use low resource scanning (reduces server load by lengthening the scan duration): Requerirá más tiempo para escanear con objeto de no sobrecargar el servidor

3º Se lanza con la opción SCAN:

Acceso en: Menú > Wordfence > Scan > Botón "Start a Wordfence scan"

Resultados: Si Wordfence muestra que hay alguna vulnerabilidad, en primer lugar deberás analizar si es un falso positivo, que suele ser lo más normal. En caso de que tu Wordpress haya sido objeto de algún ataque real, podrás intentar solucionarlo con las opciones que proporciona Wordfence.

FIREWALL

Wordfence incluye reglas para cortar conexiones que son detectadas como maliciosas. Las opciones de configuración de ataques de acceso al Escritorio por fuerza bruta son las más importantes para incrementar la seguridad. Entre ellas, se destaca configurar las siguientes opciones:

Acceso en: Menú > Wordfence > Firewall > Brute Force Protection

- **Enforce strong passwords:** Activado. Sirve para exigir uso de passwords fuertes a todos o a determinados roles de usuario
- **Lock out after how many login failures:** Bloquea (*) el acceso al Wordpress después de 20 fallos de login. Mejor reducir a 5 para incrementar la seguridad.
- **Lock out after how many forgot password attempts:** Bloquea (*) el acceso al Wordpress después de 20 fallos de recuperación de contraseña. Mejor reducir a 5 para incrementar la seguridad.
- **Count failures over what time period:** Elegir periodo para contabilizar el número de fallos permitidos. Por ejemplo, en la última hora.
- **Amount of time a user is locked out:** Tiempo en que se mantiene bloqueado el acceso a un usuario. Por ejemplo, durante 6 horas.
- **Immediately lock out invalid usernames:** Desactivado. Si se activara, en caso que te equivoques una vez al hacer login, te bloquea inmediatamente. Es una opción que incrementa la seguridad, pero cuidado, ya que puedes bloquearte el acceso con un único fallo.
- **Don't let WordPress reveal valid users in login errors:** Activado. No mostrar si el usuario con el que se ha intentado acceder era válido, para así no dar pistas a los posibles atacantes.
- **Prevent users registering 'admin' username if it doesn't exist:** Activado. Evitar que exista un usuario admin en el Wordpress, ya que es el primer nombre de usuario al que los atacantes intentarán adivinarle la contraseña.
- **Immediately block the IP of users who try to sign in as these usernames:** Bloquear la IP de alguien que intenta entrar con esos usuarios. Por ej conviene poner: admin, administrator, wordpress, user, etc.

(*) El bloqueo de acceso a Wordpress se realiza por IP, no por nombre de usuario. La IP será la dirección pública del router de conexión a Internet. Es decir, si desde tu casa (o desde tu centro educativo) te equivocas repetidas veces al escribir tu nombre de usuario y contraseña, se bloqueará el acceso desde cualquier ordenador de tu casa (o desde cualquier ordenador de tu centro educativo).



LIMITAR TRÁFICO

Podemos visualizar el tráfico que hay en el instante:

Acceso en: Menú > Wordfence > Live Traffic

Wordfence permite limitar el tráfico de datos que se genera para evitar sobrecargas y caídas.

Acceso en: Menú > Wordfence > Firewall > Rate Limiting

- **Throttle** = regular el acceso: Wordpress responderá error 503 pero se seguirá permitiendo acceso posteriormente
- **Block** = bloquear acceso definitivamente. Poner block si tienes problemas con mucho tráfico de robots
- Immediately block fake Google crawlers: Activar
- How should we treat Google's crawlers: Treat Google like any other Crawler
- If anyone's requests exceed: 240 - throttle
- If a crawler's page views exceed: 240 - throttle
- If a crawler's pages not found (404s) exceed: 30 - block, para evitar que escaneen tu sitio ante vulnerabilidades
- If a human's page views exceed: 240 - throttle
- If a human's pages not found (404s) exceed: 30 - block
- If 404s for known vulnerable URLs exceed: 15 - block

How long is an IP address blocked when it breaks a rule: 1 hora

Parámetros sugeridos obtenidos de la ayuda de Wordfence:

https://docs.wordfence.com/en/Wordfence_options?utm_source=plugin&utm_medium=pluginUI&utm_campaign=docsIcon#Rate_Limiting_Rules

Revision #8

Created 25 April 2022 08:30:03 by Equipo CATEDU

Updated 29 June 2022 13:56:17