WordPress: 10 consejos para asegurar tu sitio web

Mantén a los hackers fuera del sistema de gestión de contenido más popular del mundo

Willem L. Middelkoop
Mar. 31, 2019

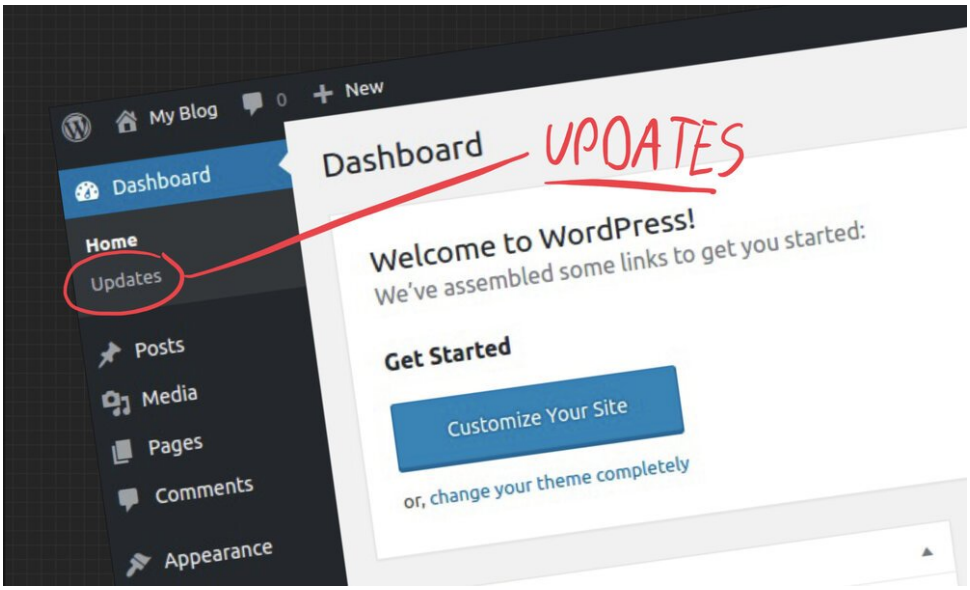
Mucha gente usa WordPress para administrar su sitio web, por lo tanto, no es sorprendente que me pidan que eche un vistazo a la seguridad de su sitio. Como hacker ético, me encuentro con WordPress en diferentes formas, tamaños y estados. Algunos de ellos están realmente mal protegidos contra hacks. Evita que tu sitio sea hackeado usando estos 10 consejos prácticos.

1) Actualizar WordPress (y plugins + temas)

La mayoría de los hackeos de WordPress son el resultado de una política de actualizaciones deficiente. Los hackers usan bots automatizados para encontrar versiones de software

obsoletas que contienen problemas de seguridad conocidos. Una vez que han descubierto que tu sitio web es vulnerable, hackearlo suele ser pan comido.

Hoy en día, la actualización de WordPress se puede hacer automáticamente, por lo que no tendrás que hacerlo tú mismo. Consulta las instrucciones sobre cómo actualizar WordPress.

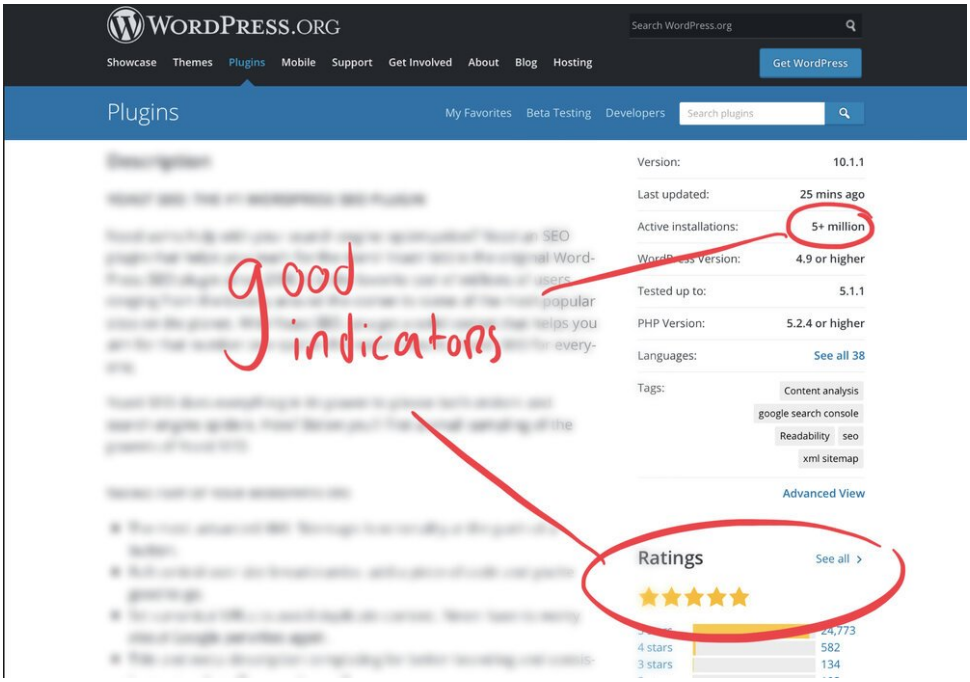


Actualizar WordPress desde el panel wp-admin

2) Plugins y Temas

La mala reputación de seguridad que se ha ganado WordPress se debe principalmente a las partes extensibles de la plataforma, específicamente los plugins y los temas. Estos son los principales vectores de ataque que explotan los ciberdelincuentes para hackear y abusar de tu sitio web de WordPress. Sus vulnerabilidades de seguridad suelen ser el resultado de errores y descuidos durante el desarrollo.

Sé muy reacio y cauteloso al instalar plugins en tu sitio web de WordPress. Debes comprobar quién es el desarrollador del plugin o tema, determinar si tiene una buena reputación en cuanto a la escritura de código seguro. Los plugins y temas con muchas descargas a menudo se mantienen activamente, un buen indicador de seguridad. Actualiza todos los plugins y temas y mantén un ojo en el historial de seguridad utilizando un sitio web como wpvulndb.com.

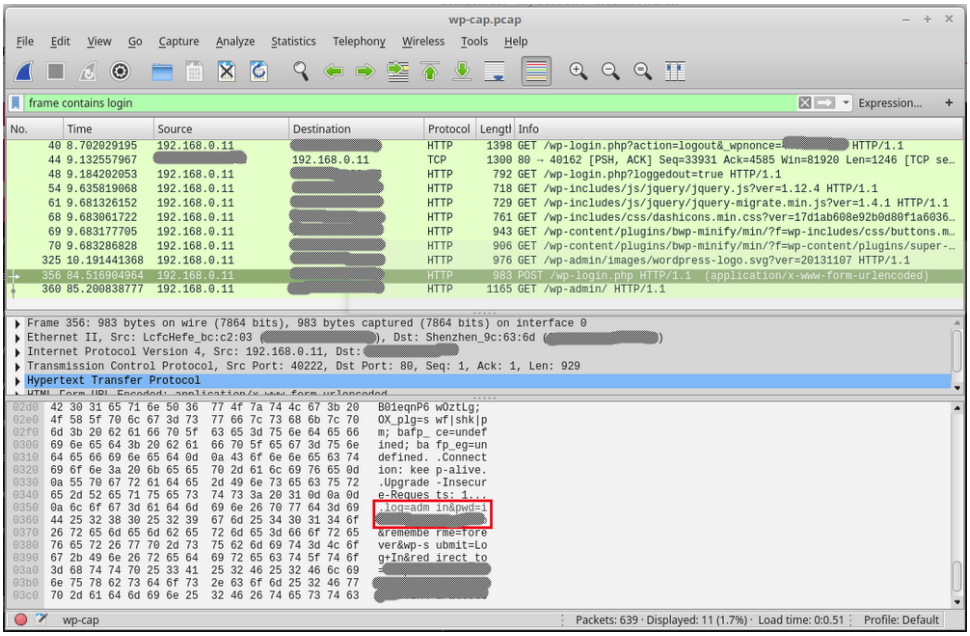


Comprobar la reputación de un plugin de WordPress mirando el número de descargas y su calificación

3) Usar cifrado (TLS/SSL)

Los sitios web de WordPress sin cifrado TLS/SSL representan un riesgo de seguridad porque cada vez que inicias sesión para administrar el sitio web, tu contraseña se envía en texto plano. Esto significa que cualquiera que esté escuchando tu tráfico de red puede obtener fácilmente tu contraseña. Con una contraseña válida, los hackers pueden simplemente iniciar sesión, no querrás ponérselo tan fácil, ¿verdad?

Usa TLS/SSL para cifrar toda la comunicación entre el servidor web y tu navegador. Eso significa que nadie puede descifrar lo que escribes en el campo de la contraseña mirando el tráfico de la red. Los certificados TLS/SSL que necesitas para habilitar el cifrado HTTPS son muy baratos en estos días, solicita a tu proveedor de hosting que obtenga uno para tu sitio.

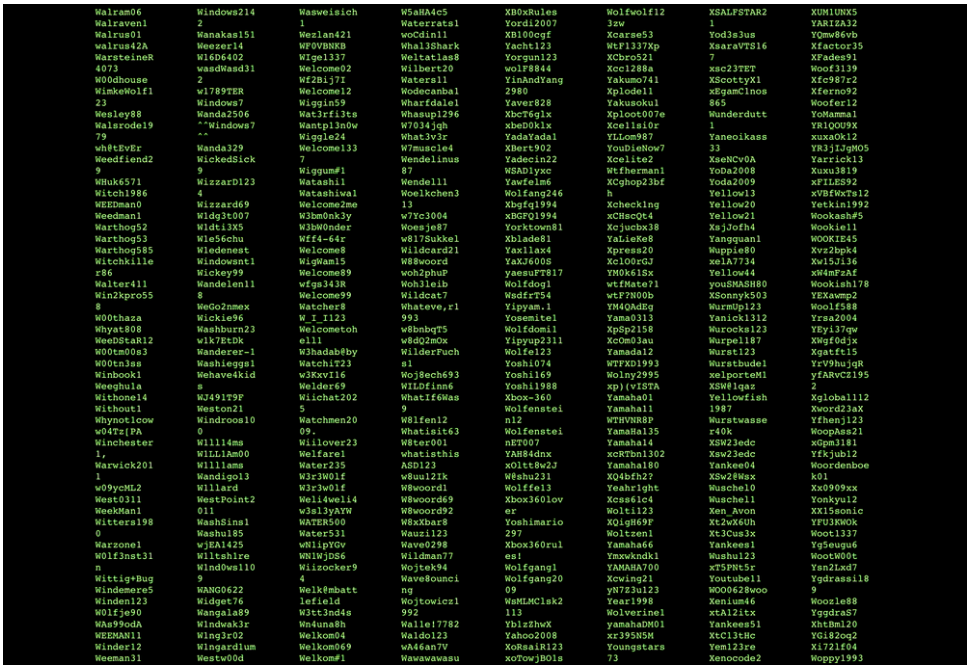


Rastrear la contraseña de WordPress usando la captura de paquetes de WireShark (vía blog.wpscans.com)

4) Usar contraseñas seguras

No importa si sigues todos los demás consejos para asegurar tu sitio web, las contraseñas débiles son otra fuente común de violaciones de seguridad de WordPress. Debido a que la mayoría de las instalaciones de WordPress tienen un usuario "admin", los hackers pueden usar diccionarios de contraseñas para adivinar automáticamente tu contraseña.

Piensa en una contraseña segura como algo que nadie haya usado antes. Esto generalmente significa más larga, con más caracteres diferentes, que no incluya palabras o frases conocidas. Puedes usar un generador de contraseñas para obtener algo realmente difícil de adivinar (y fácil de olvidar...). Evita usar la misma contraseña en varios sitios y considera habilitar la autenticación de dos pasos para un control de acceso máximo.



Walram06	Windows214	Wasweisich	W5aHA4c5	XB0xRules	Wolfwolf12	XSALFSTAR2	XUM1UNX5
Walraven1	2	1	Waterrats1	Yordi2007	3zw	1	YARIZA32
Walrus01	Wanakas151	Wezlan421	woCdinl1	XB100csf	Xcarse53	Yod3s3us	Yomv86vb
walrus42A	Weezer14	WF0VBNKB	Whal3Shark	Yacht123	WtFl337Xp	XsaraVTS16	Xfactor35
WarsteineR	W16D6402	WIge1337	Weltatlas8	Yorgun123	XCbro521	7	XFades91
4073	wasdWasd31	Welcome02	Wilbert20	wolF8844	Xcc1288a	xsc23TET	Woof3139
W00dhouse	2	WE2Bij7I	Waters11	YinAndYang	Yakumo741	XScottyX1	Xfc987r2
WinkeWolf1	wl789TER	Welcome12	Wodecanbal	2980	Xplode11	xEgamC1nos	Xferno92
23	Windows7	Wiggin59	Wharfdale1	Yaver828	Yakusoku1	865	Woofer12
Wesley88	Wanda2506	WatJrfi3ts	Whasup1296	XbcT6glx	Xploot007e	Wunderdutt	YoMamma1
Walsrode19	^^Windows7	Wantpl3n0w	W7034jqh	xbeD0klx	Xcell5i0r	1	YRiQOU9X
79	^^	Wiggle24	What3v3r	YadaYada1	YLLom987	Yaneoikass	xuxaOk12
wh@tEvEr	Wanda329	Welcome133	W7muscle4	XBert902	YouDieNow7	33	YRJjlJgMO5
Weedfiend2	WickedSick	7	Wendelinus	Yadecin222	Xcelite2	XseNCv0A	Yarrick13
9	9	Wiggum#1	87	WSADlyxc	Wtfherman1	YoDa2008	Xuxu3819
WHuk6571	WizzarD123	Watashi1	Wendell1	Yawfelm6	XCghop23bf	Yoda2009	xFILES92
Witch1986	4	Watashiwa1	Woelkchen3	Wolfang246	h	Yellow13	xVBfWxTe12
WEEDman0	Wizzard69	Welcome2me	13	Xbgfg1994	Xchecking	Yellow20	Yetkin1992
Weedman1	Wldg3t007	W3bm0nk3y	w7Yc3004	xBGFQ1994	xCHscQt4	Yellow21	Wookashd5
Warthog52	W1dt13X5	W3bW0nder	Woesje87	Yorktown81	XcjucbX38	XsjJofh4	Wookie11
Warthog53	W1e56chu	Wff4-64r	w817Sukkel	Xblade81	YaLieKe8	Yangguan1	WOOKIE45
Warthog585	W1edenest	Welcome8	Wildcard21	Yaxllax4	Xpress20	Wuppie80	Xvz2bpk4
Witchkille	Windowsnt1	WigWam15	W88woord	YaXJ600S	Xcl00rGJ	xelA7734	Xwi5Ji36
r86	Wickey99	Welcome89	woh2phuP	yaesuFT817	YM0k61Rx	Yellow44	xH4mFzhf
Walter411	Wandelen11	wfga343R	Woh3leib	Wolfdog1	wtfMate?1	youSMASH80	Wookish178
Win2kpro55	8	Welcome99	Wildcat7	WsdfrT54	wtF?N00b	XSonnyk503	YEXawmp2
8	WeGo2nmex	Watcher8	Whateve,r1	Yipyam.1	YM4QAdEg	WurmUp123	Woolf588
W00thaza	Wickie96	W_I_I123	993	Yosemite1	Yama0313	Yanick1312	Yrsa2004
Whyat808	Washburn23	Welcometoh	w8nbnbqT5	Wolfdomi1	XpSp2158	Wurocks123	YEyi17qw
WeeDStaR12	W1k7EtDk	e11	w8dQ2mOx	Yipyup2311	XcOm03au	Wurpel187	XWgfOdjx
W00tm00s3	Wanderer-1	W3hadab@by	WilderFuch	Wolfe123	Yamada12	Wurst123	Xgatft15
W00tn3ss	Washieggs1	WatchiT23	s1	Yoshi074	WTFXD1993	Wurstbude1	YrV9hujqR
Winbook1	Wehave4kid	w3XvI16	Woj8ech693	Yoshi169	Wolny2995	xelporteM1	yfARvCZ195
Weeghula	s	Welder69	WILDfinn6	Yoshi1988	xpjjvI8TA	XSW@lqaz	2
Withone14	WJ491T9F	Wiichat202	WhatIf6Was	Xbox-360	Yamaha01	Yellowfish	Xgloball12
Without1	Weston21	5	9	Wolfenstei	Yamaha11	1987	Xword23aX
Whynotlcow	Windroos10	Watchmen20	W8lfen12	n12	WTHVNR8P	Wurstwasse	Yfhenj123
w04Tz[PA	0	09.	Whatisit63	Wolfenstei	YamaHa135	r40k	WoopAss21
Winchester	Willl4ms	Wilover23	W8ter001	nET007	Yamaha14	XSW23edc	xGpm3181
1,	WILLIAm00	Welfare1	whatisthis	YAB84dnx	xcBTbn1302	Xsw23edc	Yfkjub12
Warwick201	W1lllams	Water235	ASD123	xOltt8w2J	Yamaha180	Yankee04	Woordenboe
1	Wandigo13	W3r3W01f	w8uul2Ik	W@shu231	XQ4bfh27	XSw2#Wsx	k01
w09ycML2	W1llard	W3r3w0lf	W8woord1	Wolffe13	Yeahrlght	Wuschel0	Xx0909xx
West0311	WestPoint2	Weli4weli4	W8woord69	Xbox360lov	Xcss61c4	Wuschel1	Yonkyu12
WeekMan1	011	w3el3yAYW	W8woord92	er	Wolti123	Xen_Aron	XX15onic
Witters198	WashSins1	WATER500	W8xXbar8	Yoshimario	XQigH69F	Xt2wX6Uh	YFU3KWOk
0	Washu185	Water531	Wauzi123	297	Woltzen1	Xt3Cus3x	Woot1337
Warzone1	wjEA1425	wNlipYGv	Wave0298	Xbox360rul	Yamaha66	Yankees1	Yg5eugu6
W0lf3nst31	W1ltshire	WN1WjDS6	Wildman77	es!	Ymxwkndk1	Wushu123	WootW00t
n	Windows110	Wiiocker9	Wojtek94	Wolfgang1	YANHHA700	xT5PNt5r	Yzn2Lxd7
Wittig+Bug	9	4	Wave8ounci	Wolfgang20	Xcwing21	Youtube11	Ygdrassil8
Windemere5	WANG0622	Welk@mbatt	ng	09	yN7Z3u123	WOO0628woo	9
Winden123	Widget76	lefield	Wojtowicz1	WsMLMClsk2	Year1998	Xenium46	Woozle88
W0lfje90	Wangala89	W3tt3nd4s	992	113	Wolverine1	xtAl2itx	YggdraS7
WAs99odA	Windwak3r	Wn4una8h	Walle17782	YblzZhwX	yamahaDM01	Yankees51	XhtBml20
WEEMAN11	Wing3r02	Welkom04	Waldo123	Yahoo2008	xrJ95N9M	XtC13cHc	YGi82og2
Winder12	Wingardium	Welkom069	wA46an7V	XoRsaiR123	Youngstars	Yem123re	Xi721f04
Weeman31	Westw00d	Welkom#1	Wawawawasu	xoTowjBOls	73	Xenocode2	Woppy1993

Los ataques de diccionario de contraseñas usan listas de contraseñas conocidas (filtradas), puedes encontrarlas en partes sospechosas de internet

5) Usar una computadora y una red confiables

Al igual que no debes hacer alarde de tu dinero y dispositivos en calles sombrías, debes tener cuidado dónde (y cuándo) inicias sesión en tu sitio web. Una computadora con spyware, malware o un virus puede registrar las pulsaciones de teclas (y tu contraseña) y enviárselas a los delincuentes. O incluso de una manera no digital: un adversario puede literalmente mirar por encima de tu hombro (en el autobús, tren o cafetería) mientras ingresas tu contraseña.

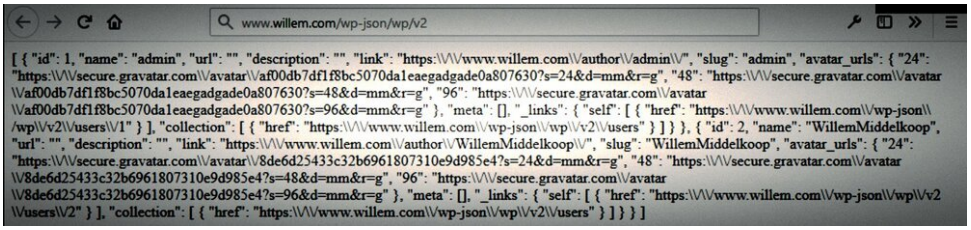
Ten cuidado dónde y cuándo trabajas en tu sitio web. No trabajes en una computadora compartida o pública cuando no sea necesario. Si trabajas con un punto de acceso WiFi público, debes usar cifrado para evitar que alguien se cuele. Puedes hacerlo usando TLS/SSL o usando una VPN (como buffered.com). Asegúrate de que tu computadora, tableta o teléfono inteligente esté actualizado.

¿Confías en el wifi gratuito que estás usando? (Imagen vía buffered.com)

6) Deshabilitar la API REST de WordPress

La API REST de WordPress proporciona acceso a todos los datos que están disponibles en tu sitio web en formato JSON legible por máquina. Se puede acceder fácilmente a publicaciones, páginas, categorías, etiquetas, comentarios, medios, usuarios, configuraciones y más. Por ejemplo, intenta agregar esta parte a la dirección de tu sitio web: **/wp-json/wp/v2/users** para obtener una lista de todos los nombres de usuario válidos de tu sitio web, *¿quieres* compartir eso con los hackers?

Deshabilita la API REST para evitar el scraping de contenido (plagio) y para evitar la filtración de datos de usuario. Los datos de usuario son personales y no deben compartirse públicamente si valoras la privacidad y la seguridad; piensa en el RGPD. Puedes deshabilitar la API REST utilizando plugins como Disable REST API o REST API Toolbox. Consulta la publicación detallada del blog de Jeff Star para obtener más información sobre cómo proteger la API REST de WP.



Filtración de información personal del usuario desde la API REST de WordPress

7) Deshabilitar el acceso XML-RPC

El XML-RPC es una función de WordPress que permite el control remoto de tu sitio web mediante XML (RPC significa "llamada a procedimiento remoto"). Este mecanismo te permite administrar tu sitio web sin iniciar sesión en WP-Admin, por ejemplo, utilizando servicios o aplicaciones externas. Desafortunadamente, la función XML-RPC es una debilidad de seguridad, ya que básicamente es una puerta trasera que los hackers pueden intentar romper mediante fuerza bruta o comandos especiales.

Evita los problemas de xml-rpc.php deshabilitando esta función de WordPress por completo. Puedes hacerlo usando el plugin Disable XML-RPC o configurando manualmente el servidor web usando un archivo htaccess.

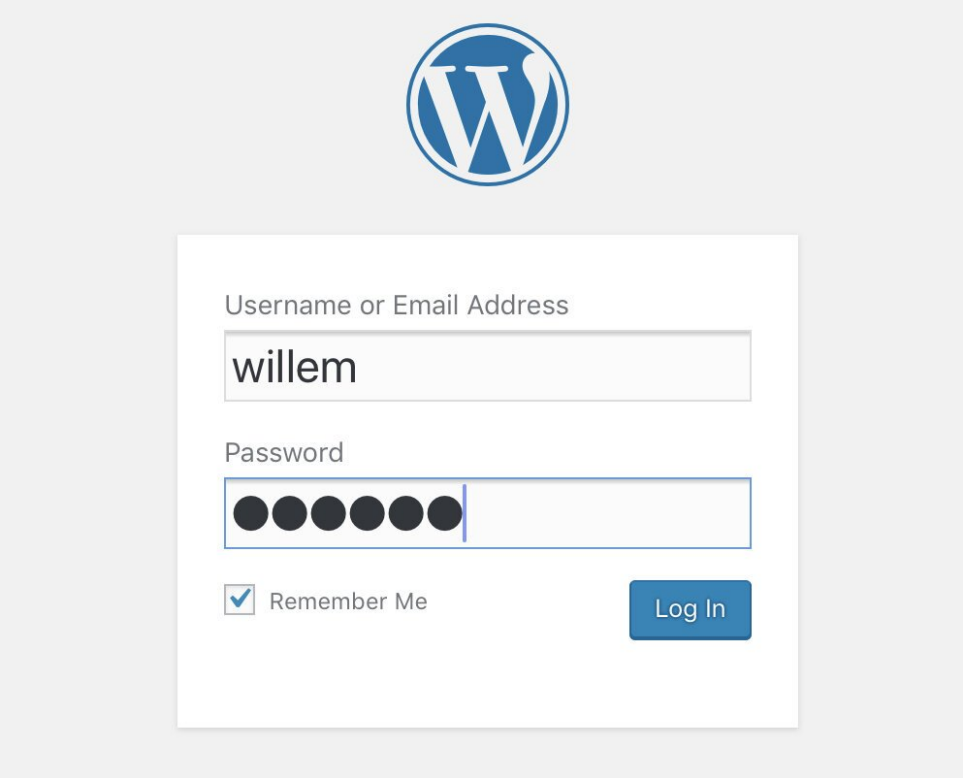
```
# Block WordPress xmlrpc.php requests
<Files xmlrpc.php>
order deny,allow
deny from all
allow from [IP]
</Files>
```

Limitar el acceso por IP a XML-RPC usando un archivo .htaccess

8) Ocultar o proteger la página de inicio de sesión (wp-admin)

Todo el mundo sabe que para iniciar sesión en WordPress, simplemente agrega '/wp-admin' a la dirección de tu sitio web. Cualquier hacker puede comenzar fácilmente con la fuerza bruta en tu sitio web debido a esto. Es mucho más difícil romper una cerradura si no puedes encontrarla.

Considera ocultar o reemplazar la página wp-admin. Los expertos llaman a esto "seguridad por oscuridad", confiando en el secreto para la seguridad. Puedes usar un plugin para esto o configurar el servidor web para limitar el acceso a wp-admin mediante el filtrado de direcciones IP. Consulta esta publicación del blog para ver formas de ocultar y proteger la página wp-admin. Sin embargo, ten en cuenta que confiar solo en el secreto no es suficiente; también debes implementar los demás consejos.



Es bastante difícil hackear mi página de WP-Admin porque no puedes encontrarla (pista: no está en /wp-admin)

9) Hosting confiable

Incluso si implementas todos estos consejos de seguridad para proteger tu sitio web de WordPress, podría no ser suficiente si tu hosting es inseguro. El hosting es el servicio que permite que tu sitio web esté disponible en Internet. Esto se hace utilizando computadoras especiales llamadas servidores. Al igual que el sitio web en sí, el servidor web que lo publica también debe ser seguro. Piensa en un hosting como un barco, si se hunde, se llevará a todos los pasajeros (sitios web) con él...

Invierte en un hosting confiable seleccionando una empresa de hosting con buena reputación. Elige uno que se adapte bien a tu empresa, considera el hosting con un VPS dedicado (administrado). Ten en cuenta que las opciones de hosting baratas a menudo son baratas porque el servidor se comparte con (muchos) otros sitios web (posiblemente

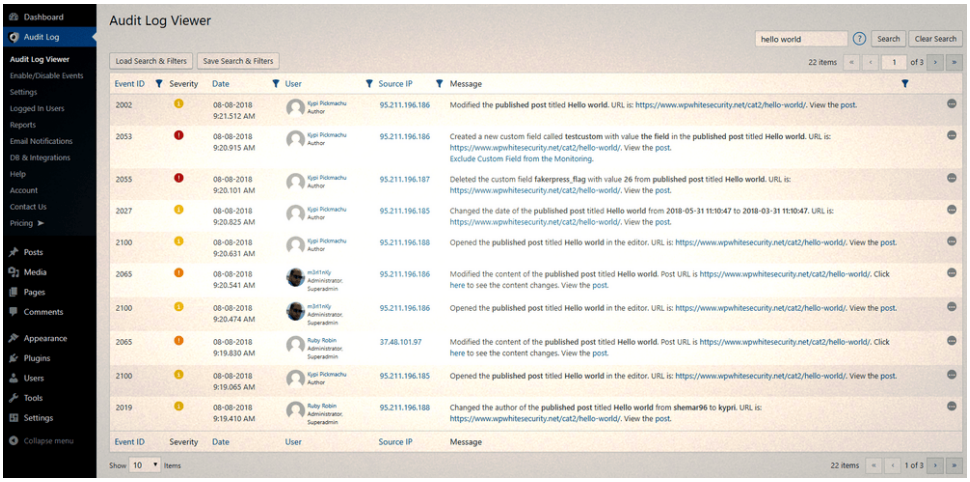
inseguros). Sigue leyendo para comprender las preocupaciones de seguridad en el hosting compartido.

En algún lugar de un centro de datos hay una máquina como esta alojando tu sitio web

10) Copia de seguridad y revisión

Aunque tu sitio web puede estar funcionando sin problemas ahora, las cosas pueden empeorar en el futuro. La seguridad nunca es algo absoluto, siempre es posible que te encuentres con mal tiempo. Prepárate para los problemas y no dejes que los problemas de seguridad pasen desapercibidos.

Revisa tu propio sitio web con regularidad, o contrata a alguien para que lo haga por ti. Con un plugin como WP Security Audit Log puedes detectar ataques y comportamientos sospechosos desde el principio. Haz copias de seguridad de tu sitio web, para que estés listo para recuperarte de un desastre cibernético. Los accidentes les ocurren a los mejores, haz una copia de seguridad de tu sitio web para evitar perder tu trabajo por completo. Consulta esta publicación del blog para aprender sobre las diferentes formas de hacer una copia de seguridad de tu sitio web de WordPress.



Usa WP Security Audit Log para vigilar lo que sucede con tu sitio web de WordPress (wpsecurityauditlog.com)

Conclusión

La seguridad de tu sitio web es como la seguridad de tu oficina o casa. Cuando te vas, cierras las ventanas y cierras las puertas, ¿verdad? No descuides la seguridad de tu sitio

web, es tan importante como su diseño y contenido.

Si implementas estos consejos de seguridad, tu sitio web será mucho más difícil de hackear por los ciberdelincuentes. Hazlo tú mismo o pide ayuda a alguien.