

WordPress: 10 tips to secure your website

Keep hackers out of the world's most popular content management system

Willem L. Middelkoop

Mar. 31, 2019

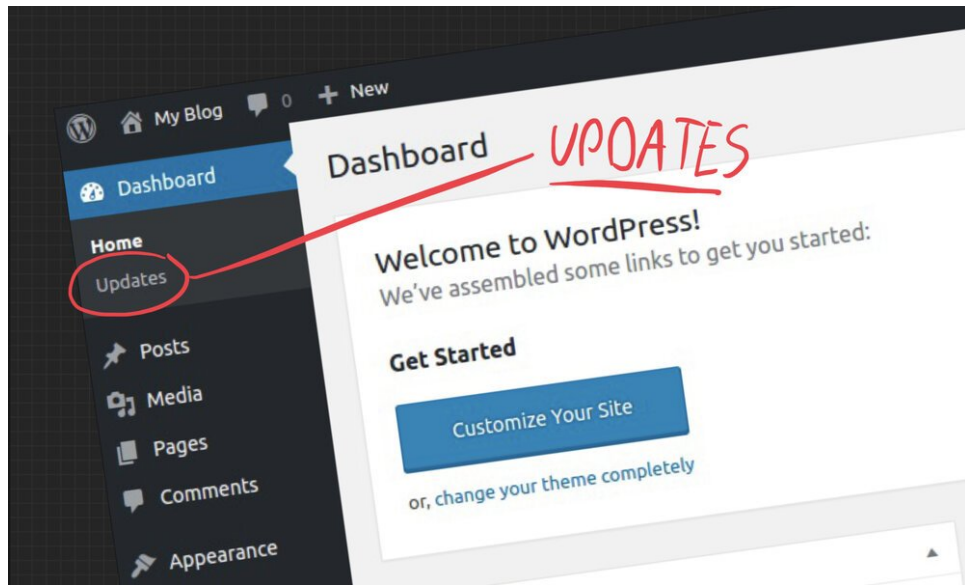


A lot of people use WordPress to manage their website, therefore it's no surprise people ask me to have a look at their site's security. As ethical hacker, I encounter WordPress in different shapes, sizes and states. Some of them are really badly protected against hacks. Prevent your site from being hacked using these 10 practical tips.

1) Update WordPress (and plugins + themes)

The majority of WordPress hacks is the result from a lackluster update policy. Hackers use automated bots to find outdated software versions containing known security problems. Once they have found your website to be vulnerable, hacking it is often a piece of cake.

These days updating WordPress can be done automatically, so you won't have to do it yourself. Check out the [instructions on how to update WordPress](#).



Update WordPress from the wp-admin dashboard

2) Plugins and Themes

The bad security reputation WordPress has earned is mostly due to the platform's extensible parts, specifically plugins and themes. These are the primary attack vectors exploited by cyber criminals to hack and abuse your WordPress website. Their security vulnerabilities are usually the result of mistakes and oversights during development.

Be very reluctant and cautious to install plugins on your WordPress website. You should check who's the developer of the plugin or theme, determine if they have a good reputation when it comes to writing safe code. Plugins and themes with lots of downloads are often actively being maintained, a good indicator for security. Update all plugins and themes and keep an eye on the security track record using a website like wpvulndb.com.

WordPress.ORG

Showcase Themes Plugins Mobile Support Get Involved About Blog Hosting

Search WordPress.org

Get WordPress

Plugins My Favorites Beta Testing Developers Search plugins

Version: 10.1.1

Last updated: 25 mins ago

Active installations: 5+ million

WordPress Version: 4.9 or higher

Tested up to: 5.1.1

PHP Version: 5.2.4 or higher

Languages: See all 38

Tags: Content analysis, google search console, Readability, seo, xml sitemap

Advanced View

Ratings See all >

★★★★★

24,773

4 stars 582

3 stars 134

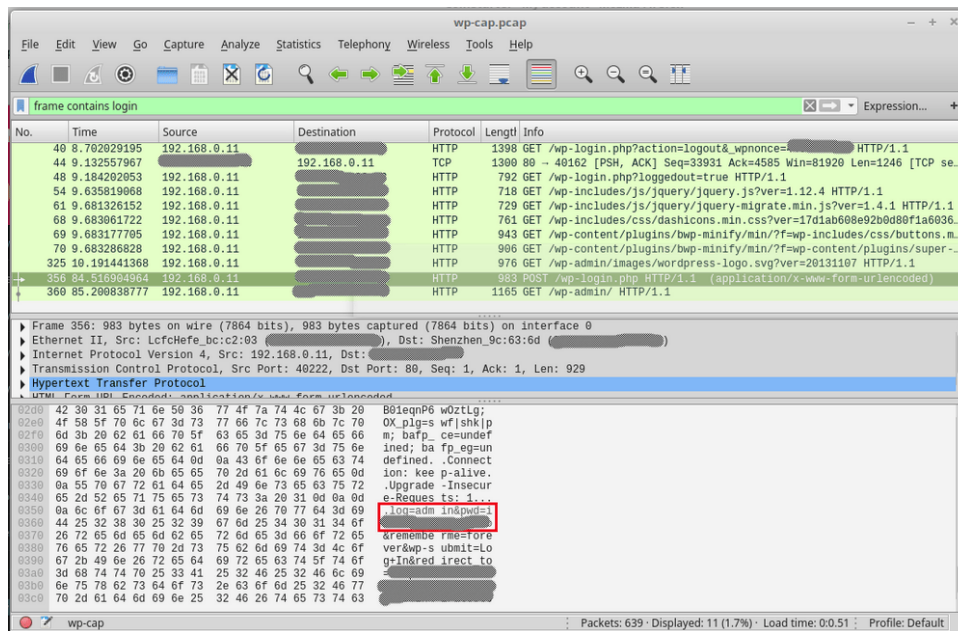
good indicators

Check the reputation of a WordPress plugin by looking at the number of downloads and its rating

3) Use encryption (TLS/SSL)

WordPress websites without TLS/SSL encryption pose a security risk because whenever you login to administer the website, your password is sent in clear text. This means that anybody that is listening to your network traffic can easily get your password. With a valid password hackers can simply login, you don't want to make it **that easy** for them, right?

Use TLS/SSL to encrypt all communication between the webserver and your browser. That means nobody can decipher what you type into the password field by looking at the network traffic. TLS/SSL certificates that you need to enable HTTPS encryption are very cheap these days, ask your hosting provider to get one on your site.



Sniff WordPress password using WireShark packet capturing (via blog.wpscams.com)

4) Use strong passwords

No matter if you follow all the other tips to secure your website, weak passwords are another common source for WordPress security breaches. Because most WordPress installations have an "admin" user, hackers can use [password dictionaries](#) to automatically guess your password.

Think of a strong password as of something that nobody has used before. This usually means longer, with more different characters, not comprising known words or phrases. You can use a password generator to get something really hard to guess (and easy to forget...). Prevent using the same password on multiple sites and consider [enabling two step authentication for maximum access control](#).

Walram06	Windows214	Wasweisich	WsaH4Ac5	XB0xRules	WolfWolF12	XSLFSTAR2	XUMIUNK5
Walraven1	1	Watterrata1	Waterata1	Yord12007	Jzw	YAR15A22	YAR15A22
Walrus01	Wanaka151	WecLan421	WecLan421	YB100cqr	Xcarse63	Yod3aBus	Yom486b
Walrus42A	Weezer14	WFOVBNKR	Whal1Shark	Yacht123	WtF1337Xp	XaaraVTS16	Xfactor35
Warsteiner	W16D6402	Wigel1337	Weltatlas8	Yorgun123	XChro521	7	Xfades91
4073	WardHead31	Welcomer2	Wellwer29	WolF4848	Xcol128a	ase212ET	Woo12139
W0Dhouse	2	Wf2B1j7f1	Waters11	YinAndYang	Yakumo741	XScottyK1	Xf987f2
WimkeWolF1	w1789TER	Welcome12	Wodecanba1	2980	Xplode11	xEGamCinos	Xferno92
23	Winecup7	Wiggin57	Wharfda1e1	Yavere888	Yakusaku1	865	Woofer12
Woolley8	W16D6402	W16D6402	W16D6402	W16D6402	Xcol128a	ase212ET	Yom486b
Wantsode19	"Windows7	W7034jgh	W7034jgh	xbeD0k1x	Xcol1a10r	1	YMOU9X
75	Wiggle24	Wiggle24	Wiggle24	YadaYada1	YLLow987	Yaneokass	xuxu0k12
W8tEYr	Wanda129	W16D6402	W16D6402	Xber1902	YoulieHow7	23	YB1212AM05
Wickedfiend2	WickedSick	7	Wendelinus	Yadecin22	Xcolite2	XseNCv0A	Yarrick13
9	WiggyuM1	87	WSD1lyxc	Wtferman1	Yoda2008	Xuxu3819	Xuxu3819
WlRuk6571	WizzarD123	Watanhil1	Watanhil1	XGghop23bf	Yoda2009	xZ11ES92	xZ11ES92
Witch1986	4	Watanhiwa1	Woolkchen3	Wolfang346	5	Yellow13	xY8W0ts12
WEDman0	Wizzard69	Welcome2me	13	Xbgfq1994	Xchecking	Yellow20	Yetkin1992
Wheedman1	Widg3k007	W3bm0nk3y	w7rc3004	XBGfQ1994	XChsCQ4	Yellow21	Wookash5
Wearthog52	W1d13X5	W3bm0nk3y	Woejeb87	Yorttcom81	Xcjcuch38	Xcjcuch38	Wookiell1
Wearthog53	W1e56chu	Wff4-64r	w817Sukkel	Xblade81	Yal1eK8	Yangquan1	WUOR1E45
Wearthog585	W1edenest	Welcome8	Wilddard21	Yaxilax4	Xpress20	Yuppie80	Xvz2bpk4
Witchhille	W1dowent1	W1g8m15	W88wood	YakJ6008	Xc100rCJ	Xc100rCJ	Xvz2bpk4
r66	W1ckey99	Welcome9	woh2phuP	YaesuF7817	YMOk618x	Yellow44	xW4mF2Af
Walter411	Wandelen11	wfgs343R	Wohl1e1b	Wolfdog1	WtfMte71	youSHASH80	Wookish178
W12kPro55	8	W16D6402	W1dcat7	Wadfrt54	WcF7W00b	XSonnyx503	YEXawmp2
8	WecO2mem	Watches8	Wateve,r1	Yinyam,1	YMOk618x	Wurmp123	Wool1588
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
WecO2mem	W111123	W111123	W111123	Wolfdom1	Xp8z2158	Wurock123	Ydy137gw
W00thaza	W1ckie96	W111123	993	Yosemite1	YMOk618x	Yanick1312	Yrsa2004
Wbyat808	Washburn23	Welcometoh	w8mbq75	Wolfdom1	Xp8z		

6) Disable WordPress REST API

The [WordPress REST API](#) provides access to all data that is available on your website in machine readable JSON format. Posts, pages, categories, tags, comments, media, users, settings and more can be easily accessed. For instance, try adding this part to your website address: `/wp-json/wp/v2/users` to get a list of all the valid usernames of your website, do you *want* to share that with hackers?

Disable the REST-API to prevent content scraping (plagiarism) and to prevent leaking user data. User data is personal and should not be shared publicly if you value privacy and security - think [GDPR](#). You can disable the REST API using a plugin like [Disable REST API](#) or [REST API Toolbox](#). Check out the [detailed blog post by Jeff Star](#) for more about securing the WP REST API.



Leaking personal user information from the WordPress REST API

7) Disable XML-RPC access

The XML-RPC is a feature of WordPress that enables remote control of your website using XML (RPC stands for "remote procedure call"). This mechanism allows you to manage your website without logging into WP-Admin, for instance using external services or apps. Unfortunately, the XML-RPC feature is a security weakness since it basically is a backdoor that hackers can try to break using [brute force](#) or [special commands](#).

Prevent xml-rpc.php problems by disabling this WordPress feature entirely. You can do this using the [Disable XML-RPC plugin](#) or by manually configuring the webserver using a [htaccess file](#).

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

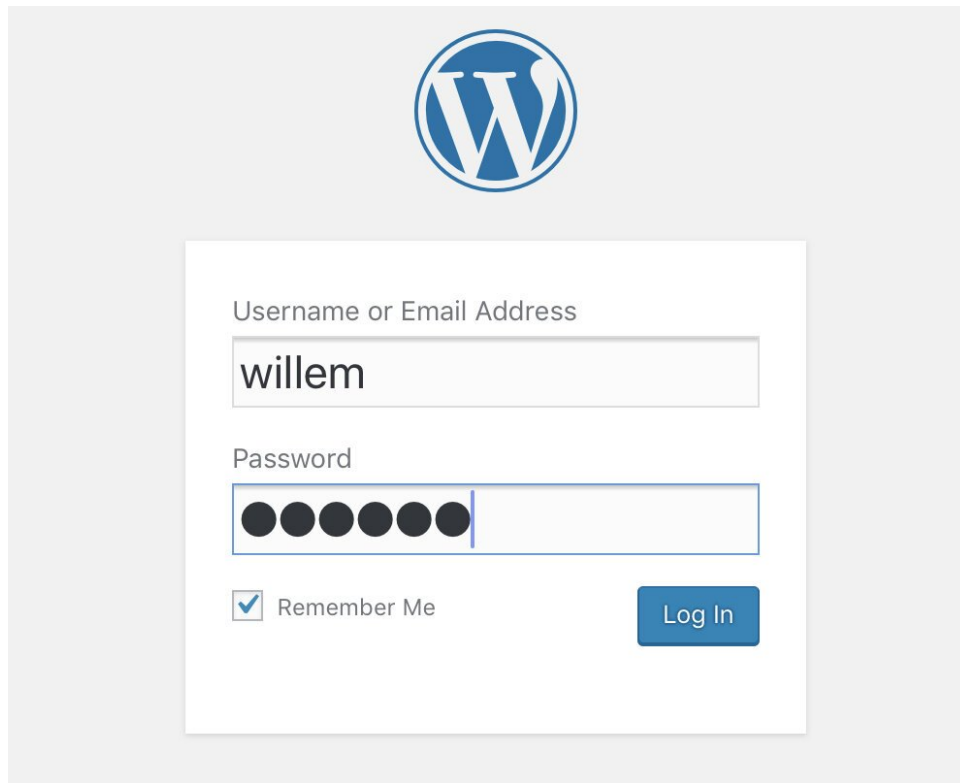
Limit access by IP basis to XML-RPC using a .htaccess file

8) Hide or protect the login page (wp-admin)

Everybody knows that to login to WordPress, you simply add '/wp-admin' to your website address. Any hacker can easily get started with brute forcing your website because of

this. It's much harder to break a lock if you cannot find it.

Consider hiding or replacing the wp-admin page. Experts call this ["security through obscurity"](#), relying on secrecy for security. You can use a plugin for this, or configure the webserver to limit access to wp-admin by IP address filtering. Check out this [blog post for ways to hide and protect the wp-admin page](#). Be warned though, relying on secrecy alone is not enough - you should implement the other tips, too.



It's pretty hard hacking into my WP-Admin page because you cannot find it (hint: it's not at /wp-admin)

9) Reliable hosting

Even if you implement all these security tips to secure your WordPress website, it might not be enough if your hosting is insecure. Hosting is the service that allows your website to be made available on the internet. This is done using special computers called servers. Just like the website itself, the web server publishing it must be secure, too. Think of a hosting as a ship, if it sinks it will take all passengers (websites) with it...

Invest in reliable hosting by selecting a hosting company with a good reputation. Pick one that fits your company well, consider hosting using a dedicated (managed) VPS. Be aware that cheap hosting options are often cheap because the server is shared with (many) other (possibly insecure) websites. Read along to [understand the security concerns in shared hosting](#).



Somewhere in a datacenter there is a machine like this hosting your website

10) Backup and backup

Although your website may be up and running smoothly now, things may change for the worse in the future. Security is never an absolute thing, it's always possible you'll run into bad weather. Prepare yourself for trouble and don't let security problems go unnoticed.

Check your own website regularly - or hire [somebody](#) to do this for you. With a plugin like [WP Security Audit Log](#) you can spot attacks and suspicious behaviour early on. Make backups of your website, so you're ready to recover from cyber disaster. Accidents happens to the best of us, make a backup of your website to prevent losing your work completely. Check this [blog post to learn about different ways to backup your WordPress website](#).

Event ID	Severity	Date	User	Source IP	Message
2002	Warning	08-08-2018 9:21:51Z AM	Karl Polmanth Author	95.211.196.186	Modified the published post titled Hello world. URL is: https://www.wpwhitesecurity.net/cat2/hello-world/. View the post.
2053	Error	08-08-2018 9:20:915 AM	Karl Polmanth Author	95.211.196.186	Created a new custom field called testtustom with value the field in the published post titled Hello world. URL is: https://www.wpwhitesecurity.net/cat2/hello-world/. View the post.
2055	Error	08-08-2018 9:20:101 AM	Karl Polmanth Author	95.211.196.187	Deleted the custom field fakagress_flag with value 26 from published post titled Hello world. URL is: https://www.wpwhitesecurity.net/cat2/hello-world/. View the post.
2027	Warning	08-08-2018 9:20:825 AM	Karl Polmanth Author	95.211.196.185	Changed the date of the published post titled Hello world from 2018-09-31 11:10:47 to 2018-03-31 11:10:47. URL is: https://www.wpwhitesecurity.net/cat2/hello-world/. View the post.
2100	Warning	08-08-2018 9:20:631 AM	Karl Polmanth Author	95.211.196.188	Opened the published post titled Hello world in the editor. URL is: https://www.wpwhitesecurity.net/cat2/hello-world/. View the post.
2065	Warning	08-08-2018 9:20:541 AM	Karl Polmanth Author	95.211.196.186	Modified the content of the published post titled Hello world. Post URL is: https://www.wpwhitesecurity.net/cat2/hello-world/. Click here to see the content changes. View the post.
2100	Warning	08-08-2018 9:20:474 AM	Karl Polmanth Author	95.211.196.186	Opened the published post titled Hello world in the editor. URL is: https://www.wpwhitesecurity.net/cat2/hello-world/. View the post.
2065	Warning	08-08-2018 9:19:830 AM	Karl Polmanth Author	37.48.101.97	Modified the content of the published post titled Hello world. Post URL is: https://www.wpwhitesecurity.net/cat2/hello-world/. Click here to see the content changes. View the post.
2100	Warning	08-08-2018 9:19:505 AM	Karl Polmanth Author	95.211.196.185	Opened the published post titled Hello world in the editor. URL is: https://www.wpwhitesecurity.net/cat2/hello-world/. View the post.
2019	Warning	08-08-2018 9:19:410 AM	Karl Polmanth Author	95.211.196.188	Changed the author of the published post titled Hello world from shemar96 to kypri. URL is: https://www.wpwhitesecurity.net/cat2/hello-world/. View the post.

Use WP Security Audit Log to keep an eye on what's happening with your WordPress website (wpsecurityauditlog.com)

Conclusion

The security of your website is just like the security of your office or house. When you leave it, you close the windows and lock the doors, right? Don't neglect the security of your website, it's just as important as its design and content.

If you implement these security tips, your website will be much harder to hack by cyber criminals. Do it [yourself](#) or ask [somebody](#) to help you.