

Advanced Blog Training

Protecting Your Website From Hackers

October 2017



By Dave Foreman



(and other CMS sites)

Hackers want to access your website to:

- Send spam mail (check at [MXToolBox.com](https://mxtoolbox.com))
- Use your site as a launch-pad to attack other sites
- Build links and install landing pages to send traffic to pharma sites
- To just plain ruin your day



(and other CMS sites)

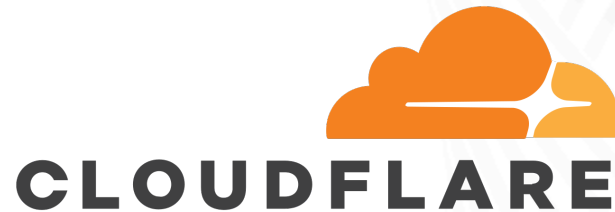
WEBSITE SECURITY

BEST PRACTICES FOR WORDPRESS

HARDEN LOG IN CREDENTIALS

1. Use a **hard password** of at least 12 characters that contains a random combination of upper and lowercase letters, numbers and symbols (we recommend using a random password generator) for your WordPress, FTP/SFTP and cPanel log ins.
2. WordPress **usernames should never be 'admin'** or 'administrator'—these are the most vulnerable usernames to attack by robots. Instead, you can use admin_dave3 or admin_14896234 (with random numbers), but not something simple admin_123.

WORDPRESS WEBSITE SECURITY

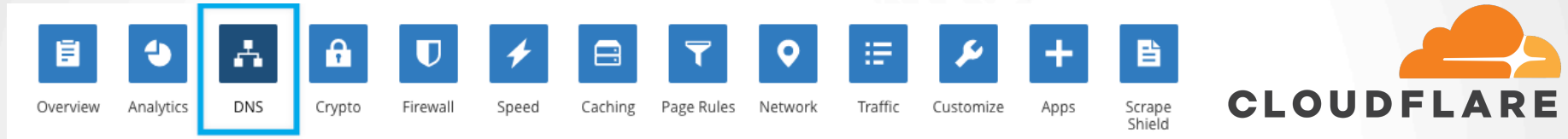


IT'S A VERY VALUABLE TOOL!

Cloudflare is a great way to make your WordPress site work better in terms of page load time and it helps to fend off attacks. **It should be used on every website! It's free, and provides some level of security even if you don't update the settings. Cloudflare caches images, blocks automated scripts and acts as firewall**

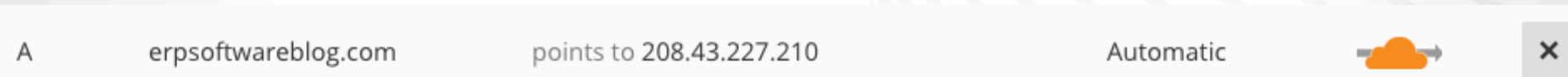
Note Joomla, Drupal and other CMS's are very vulnerable to attacks. You should use Cloudflare and adapt your Cloudflare settings for these sites. Contact us for further assistance with this as this presentation is primarily for WordPress websites.

(Cloudflare settings can be applied to ExpressionEngine and Joomla sites in some cases)



CACHING YOUR WEBSITE

Caching your website enhances the site's speed and performance.
Anything in Cloudflare that goes to website should use caching.



If you are making changes to the website and it's cached, you will want to put the site into Development mode so you can see your changes as you make them. After 3 hours, this setting should revert back automatically.

Overview > Quick Actions > Development Mode

WORDPRESS WEBSITE SECURITY



Overview



Analytics



DNS



Crypto



Firewall



Speed



Caching



Page Rules



Network



Traffic



Customize



Apps



Scrape
Shield



CLOUDFLARE

Scrape Shield

Protect content on your site.

Email Address Obfuscation

Obfuscated email addresses displayed on your website to prevent harvesting by bots and spammers, without visible changes to the address for human visitors.

This setting was last changed 10 months ago

On

Server-side Excludes

Automatically hide specific content from suspicious visitors.

This setting was last changed 10 months ago

On

SCRAPE SHIELD

Good for any website.

The email address obfuscation setting will make emails invisible to most email bots. If you have an email listed on your website, like on the contact page, turn this on so that the email isn't visible to robots.

WORDPRESS WEBSITE SECURITY



Security Level

Adjust your website's Security Level to determine which visitors will receive a challenge page.

This setting was last changed 10 months ago

Medium

[API](#) [Help](#)

Challenge Passage

Specify how long a visitor with a bad IP reputation is allowed access to your website after completing a challenge. After the Challenge Passage TTL expires the visitor in question will have to pass a new Challenge.

This setting was last changed a few seconds ago

30 minutes

[API](#) [Help](#)

FIREWALL

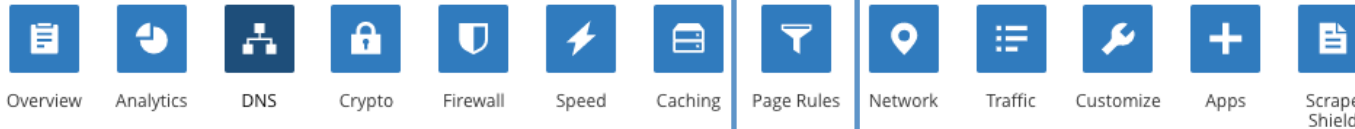
Security should be set to medium for extra protection.

Challenge passage should be 30 min as set by default.

An IP address could be from a foreign country and Cloudflare is constantly finding bad IP's and blocking them.


Cloudflare may show a page asking someone if they are a human and they will have to check a box if the IP address is deemed as dangerous.

WORDPRESS WEBSITE SECURITY



PAGE RULES

Browser integrity check: detects if a real human with a real browser is attempting to log in to the website. This protects against a brute force attack where robots repeatedly hit your website and attempt to log in repeatedly.




yourwebsite.com/wp-login

Then the settings are:

Browser Integrity Check	On
Security Level	I'm Under Attack

Security level: all this does is create a delay screen. Even if it's a sophisticated robot, every time it hits your site it has to wait 5 seconds. Also prevents an overload because of the constant hits and will prevent from your site going offline.



(Note: for Joomla sites you would use /administrator instead of /wp-login)

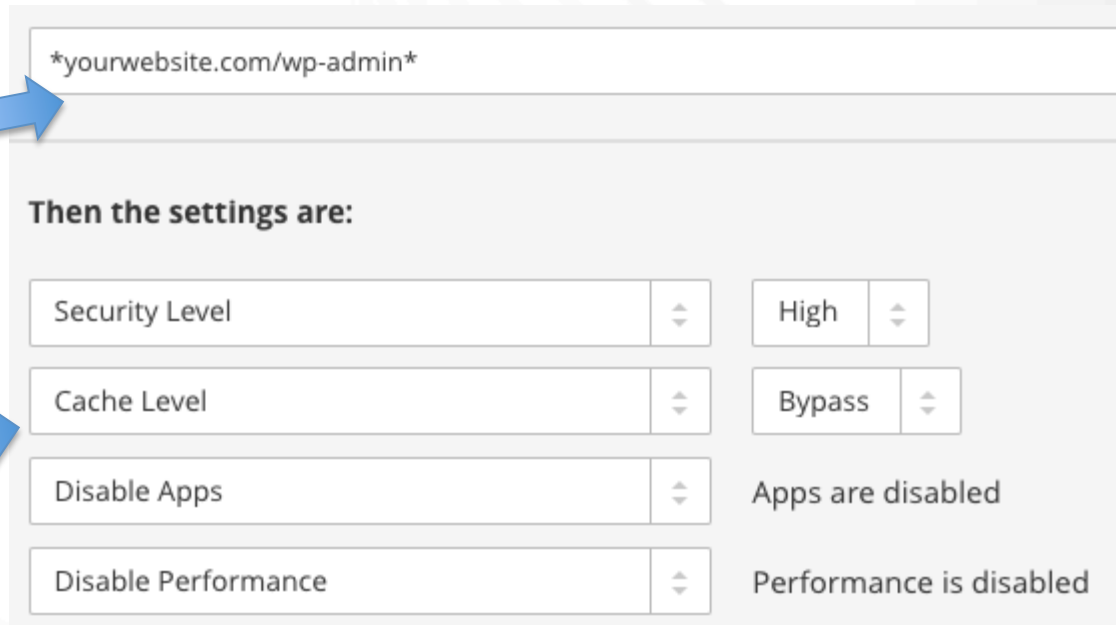
WORDPRESS WEBSITE SECURITY



PAGE RULES

wp-admin redirects to the wp-login page we already set a rule for. Make sure to include stars.

You don't want the backend of your website to cache when you are logged in to your admin panel. 'Disable apps' makes sure that Cloudflare does not interfere with the backend of your website.



yourwebsite.com/wp-admin

Then the settings are:

Security Level	High
Cache Level	Bypass
Disable Apps	Apps are disabled
Disable Performance	Performance is disabled

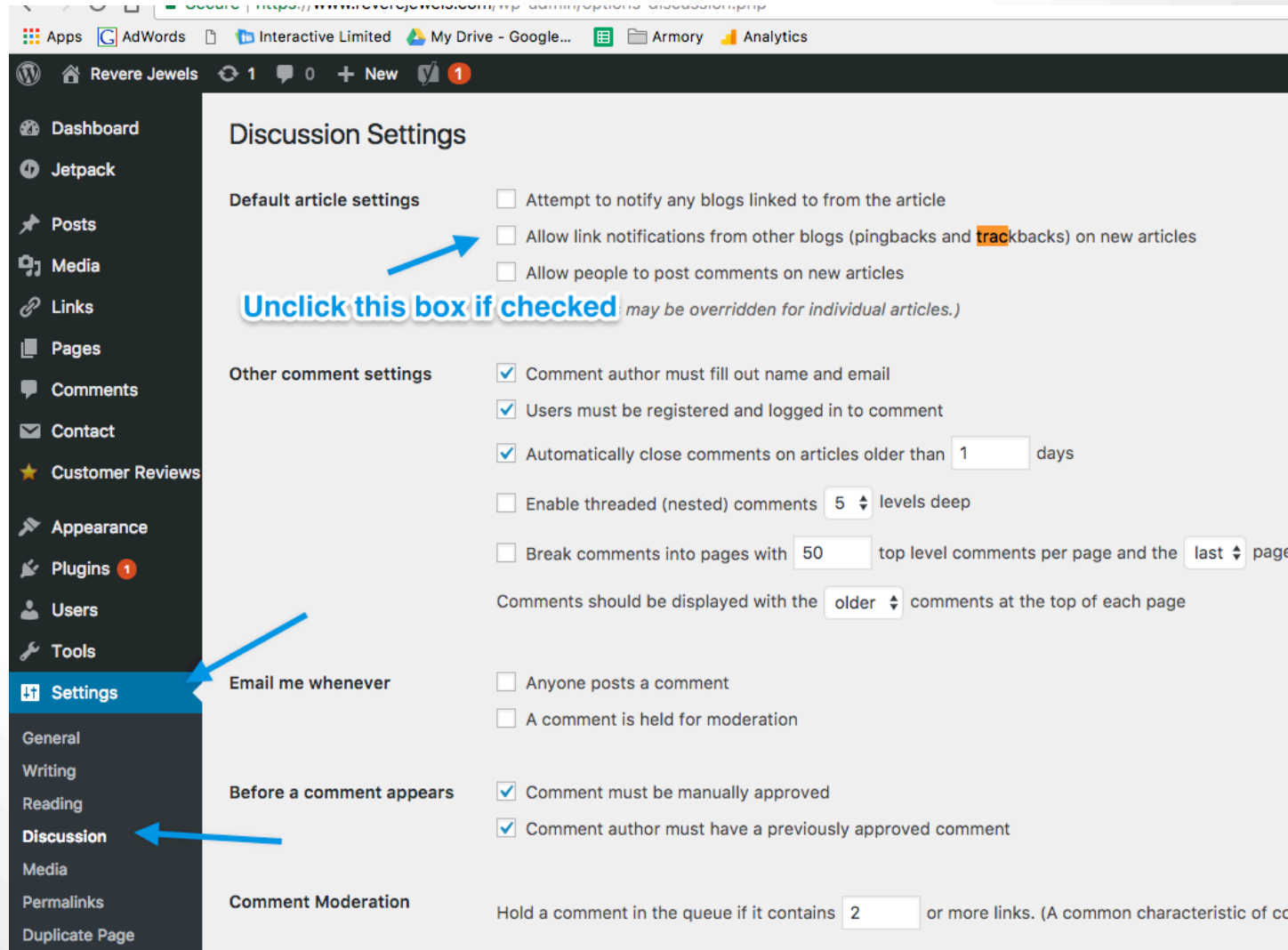
You can watch this video to learn more about page rules in Cloudflare:
<https://www.cloudflare.com/features-page-rules/optimize-wordpress/>

BEST PRACTICES FOR WORDPRESS

DISABLE PINGBACKS

Just make sure this box is unchecked as indicated in the screenshot:

Settings >
Discussion





PROTECT YOUR WORDPRESS WEBSITE!

Wordfence is a free plugin for WordPress websites. This security plugin sends you messages when something suspicious is happening with your website and scans plugins. We recommend everyone with a WordPress site install Wordfence and use the default settings.

RUN THE INITIAL WORDFENCE SCAN UPON INSTALLATION

If you want special settings, contact us for more details.

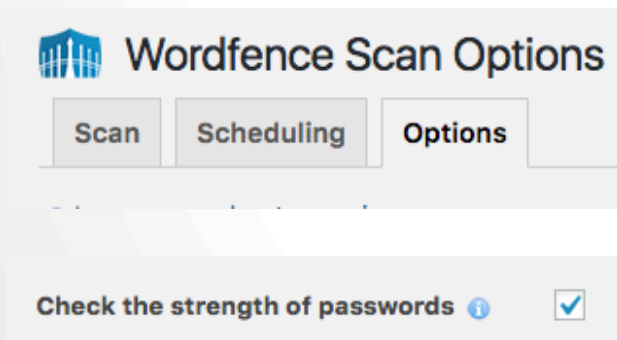
WORDPRESS WEBSITE SECURITY



ENTER AN EMAIL ADDRESS FOR SOMEONE ACTIVE IN YOUR COMPANY WITH ACCESS TO YOUR WEBSITE

WordPress will warn you if you use a plugin that hasn't been updated in awhile. Put an email address in Wordfence for these types of warnings so that someone will fix these types of vulnerabilities. To prevent your inbox from getting overwhelmed with notifications, there is an option in Wordfence to check a box for serious issues only. This is the setting we recommend.

WORDPRESS WEBSITE SECURITY



Make sure this box
is checked under
the scan options



PASSWORD AUDITING

Run the Wordfence password audit to see which website users have an weak password. Once the audit is complete you will see the results and have the ability to change weak passwords yourself and have the new password emailed to the site user. Alternatively you can send your users and administrators a request that they change their password themselves.

AVOID VULNERABLE PLUGINS

THIS APPLIES TO BOTH WORDPRESS AND JOOMLA WEBSITES

Always be careful when installing plugins! Only use plugins that have thousands of installs, reviews, and are updated regularly (within the past couple of months). Plugins can have vulnerabilities that make them very easy to hack—thus making your website easy to hack. There is no protection when you download a badly written plugin. These create big security gaps in the website so make sure to fully investigate a plugin prior to installing it.

If you have a choice of whether to use a plugin or not, DON'T, because it could create vulnerabilities.

BEST PRACTICES FOR WORDPRESS

UPDATE PLUGINS

You need to check your WordPress plugins monthly for updates. If a plugin has an update available, make sure you install the update.

Hackers exploit plugins that have not been updated

Whenever possible set your plugins to auto-update.

BEST PRACTICES FOR WORDPRESS

USE A PREMIUM HOST FOR YOUR WORDPRESS SITE

The price you pay for hosting reflects what you get. Don't use GoDaddy for hosting, or other cheap providers. The price of a premium host will be \$20+ per month.



These hosts are faster, use their own caching and have their own security measures. Some premium hosting sites do not allow Wordfence because they provide their own security system. Make sure you still use Cloudflare to help the performance of the site, prevent hackers and block bad IP addresses.

BEST PRACTICES FOR WORDPRESS

USING YOUR OWN DEDICATED SERVER

If you are hosting your website on your own dedicated server it is VERY important to use Cloudflare and Wordfence (or All-in-One Security and Firewall).

Most dedicated servers aren't built with adequate security measures in place for WordPress websites.

BEST PRACTICES FOR A SECURE WEBSITE



DOMAIN NAME REGISTRAR

Where is your domain name registered? Is your password secure?

Make sure the domain lock is on for your domain name. It is possible for someone to steal your domain name. A secure password and domain lock will help to prevent this from happening.

This also prevents someone from logging in and changing settings for your domain, or sending out emails from your domain that you don't know about.

BEST PRACTICES FOR MONITORING WEBSITE UPTIME



UptimeRobot is free will alert you to a hack. Oftentimes, when a website is attacked the site will go down.

This is a good thing to have in place to alert you if your website goes down due to any issue.

Setup two tests, an http test, and a keyword test. If you have a separate site for mobile (WP Touch) you will want to email them and have them setup a test using a mobile browser user agent.

BEST PRACTICES FOR EMAIL DELIVERY & FORM SUBMISSIONS

Using Postmark App is important!




Why do you need to use Postmark App?

Postmark validates emails coming from your website. It will shut down hackers from taking over your website and using it to send out emails. Postmark App also guarantees delivery of emails coming from forms on your website. **Use Postmark so you don't miss any leads.**

ISPs and service providers will often block leads that aren't coming from an email client but instead by a website form, since most spam emails are sent from websites. Hackers look for websites and servers to attack to send emails.

Setup requires some technical knowledge. For assistance with setup, contact Interactive Limited.

 **SendGrid** is an alternative to Postmark

BEST PRACTICES FOR MONITORING WEBSITE HACKING



SUCURI [offers a free scan](#) to let you know if your website has been hacked. Your site can look and work fine and unexpectedly have tons of links to a pharmaceutical drug on a sub domain you didn't even know existed.

We recommend you run this scan once a quarter even if you have the Wordfence plugin, or if you think your site has been hacked. Some indications that your site has been hacked are: plugins turning themselves off, site running slow, emails bouncing or messages being sent that you never sent.



WORDPRESS HOSTING & SUPPORT

**[CHECK OUT INTERACTIVE LIMITED's MONTHLY WEBSITE
MAINTENANCE PLAN](#)**

**IF YOU WANT THE REASSURANCE OF KNOWING YOUR WEBSITE IS
PROTECTED AND MAINTAINED REGULARLY**

From hosting to website maintenance, website security, SEO advice
and more, we've got you covered!

WEBSITE SECURITY – Static Websites

If you have a static website instead of a WordPress website, your site is at a lower risk for hacking. Follow these simple guidelines to secure your website:

1. Make sure your FTP logins are SFTP
2. Use a hard password of at least 12 characters that contains a random combination of upper and lowercase letters, numbers and symbols (we recommend using a random password generator) for your FTP/SFTP and cPanel log in

For questions, contact:

David Foreman

dave@interactivelimited.com

Brittany Farley

brittany@interactivelimited.com

Phone: 888-800-0999

RESOURCES YOU CAN USE TO LEARN MORE

You can watch this video to learn more about page rules in Cloudflare:
<https://www.cloudflare.com/features-page-rules/optimize-wordpress/>

Learn more about Wordfence password auditing here:
<https://www.wordfence.com/blog/2015/04/wordfence-announces-password-auditing/>

*Good site for checking email server hacking: <https://mxtoolbox.com>
They have a subscription service that will check monthly*

Check out our monthly website maintenance plan: <http://s.illlc.com/cxSlq8>