

WordPress Security Best Practices

Niagahoster Virtual Summit 2019

Ivan Kristianto
ivan@ivankristianto.com



Ivan Kristianto **(ivan@ivankristianto.com)**

Senior Web Engineer at 10up

Google Developer Expert for Web Technology

WordPress Jakarta Meetup Organizer

WordCamp Asia 2020 Organizer



What I heard From People

WordPress is Not Secured

naked security by SOPHOS

Award-winning computer security

WordPress backdoored

WordPress XSS Bug Allows Drive-By Code Execution

fake admin



Author:
Tara Seals

September 13, 2019
/ 4:52 pm

minute read

Write a comment

Share this article:



fake admin accounts

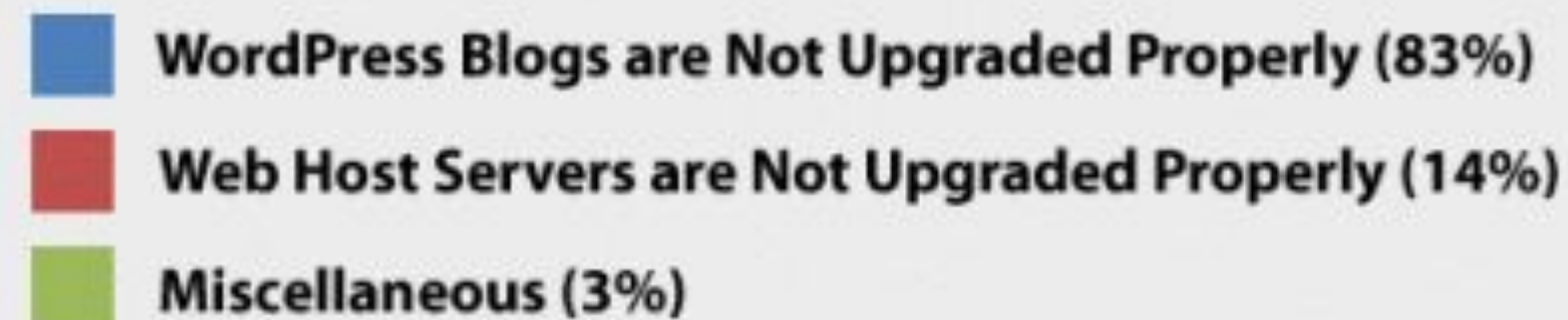
Sites that use the Gutenberg (found in WordPress 5.0 to 5.2.2) are open to complete takeover.



What I Understand

WordPress is as secured as how much you understand your site

83% of Hacked WordPress Blogs are not upgraded.



The chart displays the possible reasons why WordPress blogs were hacked and the study concludes it was mostly because they were not running the most upgraded version of WordPress.

To Keep Your Blog Secure, You Must

Stay Updated with New Releases

You must keep up with each major release and each security releases. Subscribe to WordPress blog, or WPBeginner to get timely updates on each new release.

Keep Your Plugins Upgraded

Each Plugin can be vital for your blog's security. Upgrade plugins as soon as the author releases a newer version because they also release the bug fix report which can be hacker's best asset.

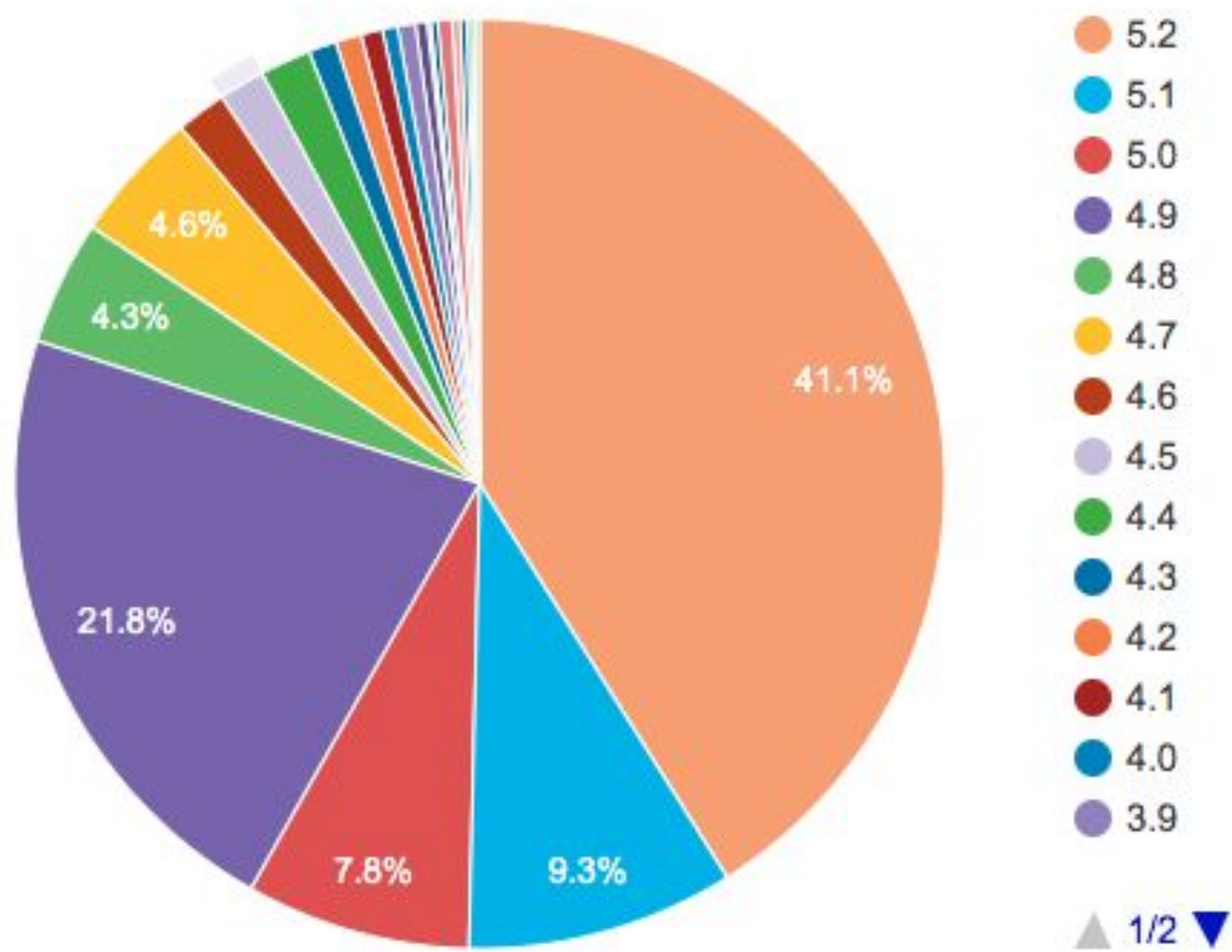
Pick a Reliable Webhost

Reliable webhost can make a huge impact on your blog's security. A reliable host keep their server's updated with each new software release thus increasing your site performance and safety.

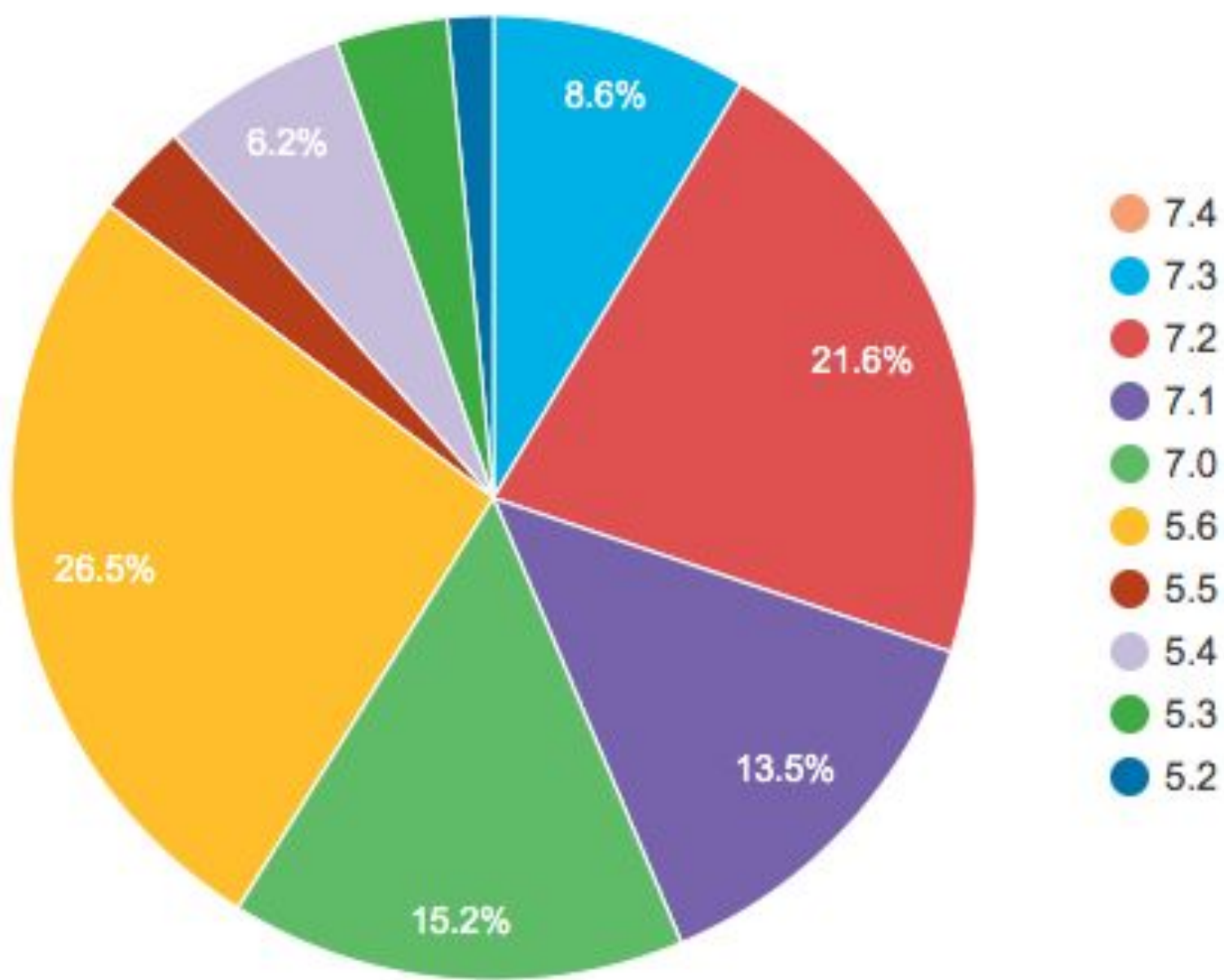


WordPress & PHP Version

WordPress Version



PHP Versions



<https://wordpress.org/about/stats/>



Steps to Security Best Practices



Step #1

Always Use HTTPS



HTTPS is free with Let's Encrypt™ SSL

Let's Encrypt™ SSL

Let's Encrypt™ is an effort to provide free domain-validated certificates in an automated fashion. This page provides a facility to issue certificates via the Let's Encrypt™ service. Certificates issued here will be renewed automatically. Service status: Operational ●

[View settings](#)

Your domains with Let's Encrypt™ certificates

Show 10 entries

Search:

Domain	Alt Names	Status	Validation	Expiry	Actions
14.wpjktmeetup.com	14.wpjktmeetup.com www.14.wpjktmeetup.com	Installed	http-01	11 Jan 2019	Remove Reinstall View
blog.wpjktmeetup.com	www.blog.wpjktmeetup.com	Installed	http-01	10 Jan 2019	Remove Reinstall View
shop.wpjktmeetup.com	www.shop.wpjktmeetup.com	Installed	http-01	10 Jan 2019	Remove Reinstall View

cPanel > Let's Encrypt™ SSL

Related Links


- <https://letsencrypt.org/>



Step #2

Use PHP 7.2 or Above



 MultiPHP Manager



System PHP Version


The system default PHP version is set by the system administrator.
Any domain that is set to the *inherit* value indicates that it does not have its own PHP version explicitly set. Read more about [inherit](#).


ea-php56

Set PHP Version per Domain








Select the domains that you wish to change from the table, then apply a PHP version from the list.

PHP Version alt-php44  



Selected 

Showing 1 - 5 of 5 items

<input type="checkbox"/>	Domain ▲	PHP Version	PHP-FPM
<input type="checkbox"/>	*.wpjktmeetup.com	ea-php71	
<input type="checkbox"/>	14.wpjktmeetup.com	ea-php71	
<input type="checkbox"/>	blog.wpjktmeetup.com	ea-php56 	
<input type="checkbox"/>	shop.wpjktmeetup.com	ea-php56 	
<input type="checkbox"/>	wpjktmeetup.com	ea-php56	

cPanel > MultiPHP Manager

YouTube Videos

- PHP in 2017 - Rasmus Lerdorf @ WeAreDevelopers Conference 2017



Step #3

Use WordPress Auto Update



83% of WordPress Hacked are not upgraded. And WordPress has auto update feature.

- WordPress Core Auto Update
 - `define('WP_AUTO_UPDATE_CORE', true);`
- WordPress Plugin Auto Update:
 - `add_filter('auto_update_plugin', '__return_true');`
- WordPress Themes Auto Update
 - `add_filter(auto_update_theme, '__return_true');`

Related link

- <https://wordpress.org/support/article/configuring-automatic-background-updates/>



Step #4

Use Strong Username and Password

8% of the WordPress hacked because of weak username and password. Here are some practice you can follow:

- Security through obscurity
 - Use random username, such as *technoj4rafy6kbm, ivlsle888*
- Use strong password
 - minimal 16 random characters
 - Use uppercase, lowercase, number and symbols
 - Sample: *NkdW4#XWUDV7eN6Q, aU4f@X.FkT_GWb4a*
- Use password manager:
 - 1Password (Not Free)
 - LastPass (Free/Paid)



Related link

- <https://themeisle.com/blog/wordpress-image-optimizer-plugins-compared/>



Step #5

Use 2 Factor Authentication

Add 2FA to your site will add an extra security layer, and it is very recommended. Here are some way to do it:

- Use WordPress.com login authentication, it has 2nd factor authentication. Connect using [Jetpack Plugin](#).
- Or use plugin two-factor:
<https://wordpress.org/plugins/two-factor/>



Related Links

- <https://jetpack.com/support/sso/>



Step #6

Download Plugins/Themes from the original source



There are many nulled and hacked plugins shared on the internet.

Don't use them!

Always download plugins/themes from their original source.

Here are some reasons:

- Avoid from getting malware or unwanted code
- You can get support from the author or the community
- The source code is always open / not encrypted

WordPress Repo

- <https://wordpress.org/plugins/>
- <https://wordpress.org/themes/>



Step #7

Limit User Access

Most of the time we don't know who install the plugins or change the themes. This due to too many administrator on the site.

- Limit number of Administrator
 - Good practice for small site, it should not have more than 3 administrators
- Other user choose between Editor or Author
- If you create custom role, exclude anything related to plugins/themes for this custom role. Only Administrator should has that capabilities



Related Link

- <https://wordpress.org/support/article/roles-and-capabilities/>



Step #8

Firewall

Use correct settings of Firewall could add many benefits to prevents attack to your site. Here are some best practice I do:

- Protect wp-admin folder
 - Use server-side password protection, with basic-auth
 - Or, protect wp-admin access only from your IP address / VPN IP address
- Use one of the proxy service below will give you extra security from bot / brute force attack:
 - Cloudflare
 - Sucuri
 - Incapsula

Secure your server



Related Link

- <https://www.cloudflare.com/>



Step #9

File and Folder Permission



Set the correct file and folder permission in your server will give hard time for the attacker to inject your site.

- Setting File Permission

- `find /path/to/your/wordpress/ -type d -exec chmod 755 {} \;`
- `find /path/to/your/wordpress/ -type f -exec chmod 644 {} \;`

- Securing [wp-includes](#)

- Securing [wp-config.php](#)

- Disable File Editing

- `define(DISALLOW_FILE_EDIT, true);`

Read more

- <https://wordpress.org/support/article/hardening-wordpress/#securing-wp-includes>
- <https://wordpress.org/support/article/hardening-wordpress/#securing-wp-config-php>



Step #10

Code Audit for Plugins/Themes



Before install or update plugin/themes, it is a good practice to run code audit, and here are some best practice:

- No encrypted code
- Code should not download any other code from 3rd party
- Code should not send any kind of information to 3rd party
- Code should always sanitize all input
- Code should always escape all output
- Code should implement nonces for every input
- Check wpvulndb.com for extra precautions.

Links

- <https://10up.github.io/Engineering-Best-Practices/php/#security>
- https://codex.wordpress.org/Validating_Sanitizing_and_Escaping_User_Data



Step #11

Disaster Recovery Plan



Add plan for disaster recovery for your site will give you some peace of mind when something happen to your site.

Here are some useful practice:

- Every shared hosting with cPanel will have backup plan for each day, week and month. Contact your hosting support to enable this.
- Use one of this WordPress plugin:
 - Vaultpress (Jetpack Backup): Paid
 - UpdraftPlus: Free, and Paid for Premium version
 - BackWPup: Free, and Paid for Pro version
 - Duplicator: Free
 - All-in-One WP Migration: Free



Thank You!

