



# How Hackers Exploit Websites with Pending Updates

W O R D C A M P   M S P   2 0 2 0



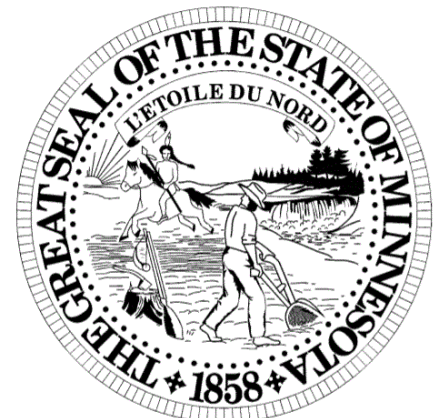


# Hi, I'm Nick Wolfe

---



THOMSON REUTERS

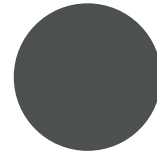




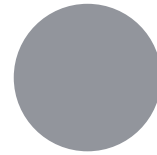
# Goals

- ✓ Empower you to keep your website safe through regular updates.
- ✓ Demystify website hacking
  - Provide strategies for managing
- ✓ updates for WordPress core, plugins, themes, and PHP

# What is an ethical hacker?



Inspects infrastructure for security vulnerabilities.

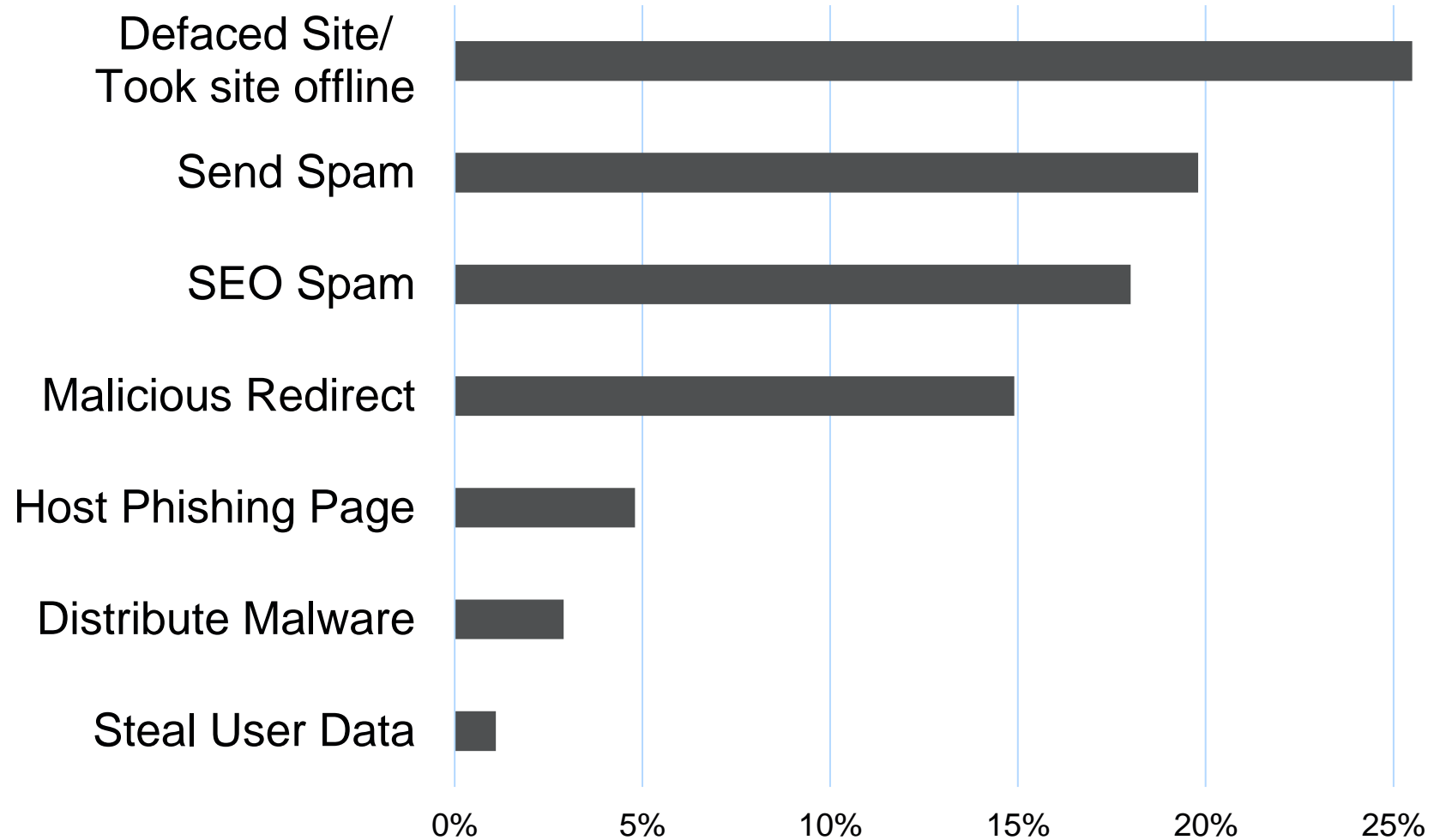


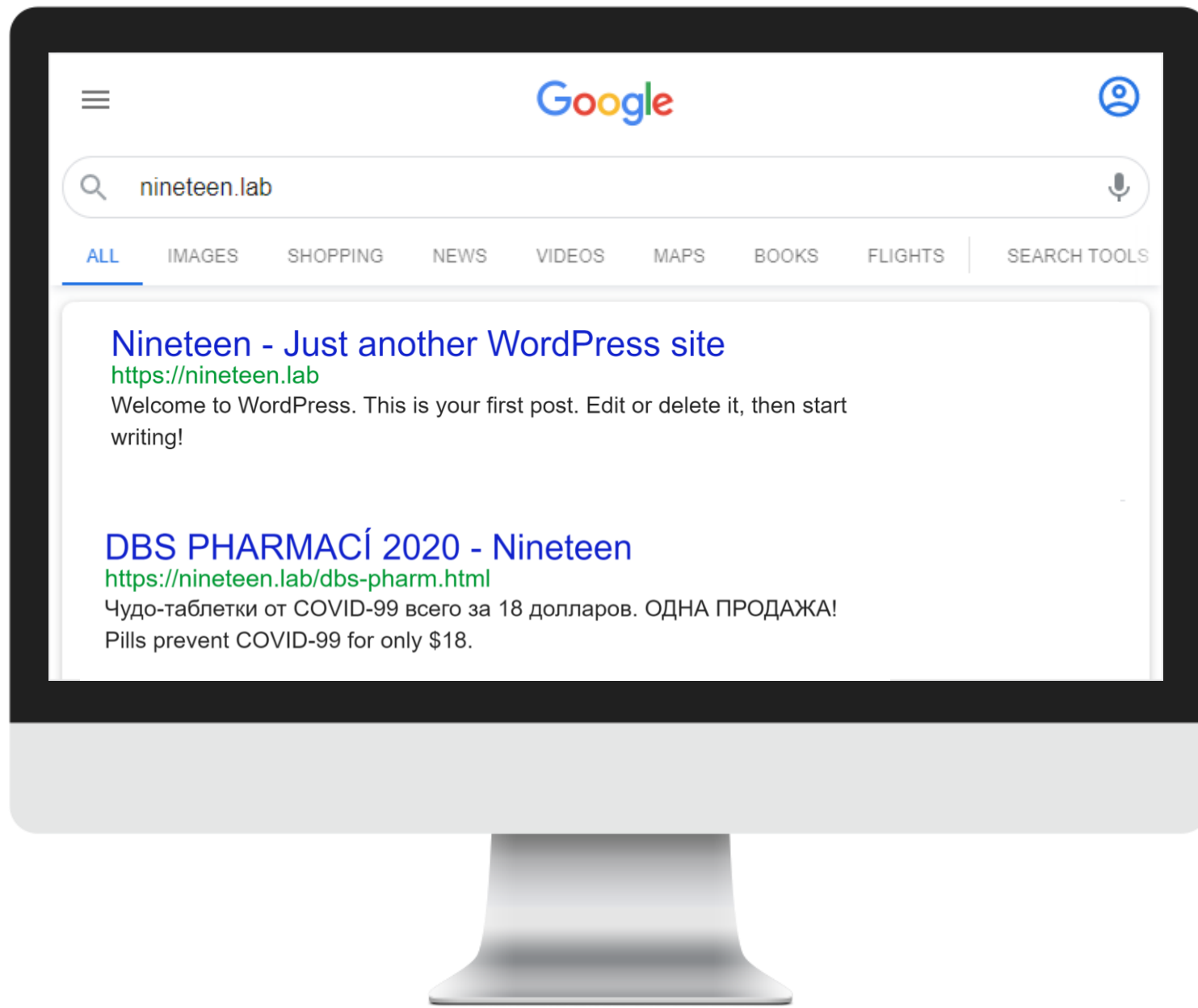
Has consent of the owner of the infrastructure.



Also referred to as “white hat” hacking.

# Why do hackers hack?





SEO  
Spam

WordPress 3.9-5.1 - Comment Cr x

+

←

→

↺

https://wpvulndb.com/vulnerabilities/9230


☆

🔒

📁

👤

⋮



[WordPress](#) [Plugins](#) [Themes](#) [API](#) [Submit](#) [Login](#) [Register](#)

SEARCH

# WordPress 3.9-5.1 - Comment Cross-Site Scripting (XSS)

Description

According to WordPress:

"This release also includes a pair of security fixes that handle how comments are filtered and then stored in the database. With a maliciously crafted comment, a WordPress post was vulnerable to cross-site scripting."

## Affects WordPresses



# Demonstration

W O R D P R E S S   C O R E   X S S

3 . 9   T O   5 . 1



# Solutions

- ✓ Update WordPress

This has been patched since 2019, so ensure your website is up to date.

- ✓ Be careful what you click!

Don't open suspicious links.

If you must open the link, log out of WordPress or use an Incognito window in your browser.

- ✓ Turn off 'X Frame Options'

Turn off 'X Frame Options' for HTTP requests to prevent clickjacking.

Sometimes hosts or plugins will do this by default.

- ✓ Install a web application firewall.

Wordfence is a good option.

# WordPress Core: Automatic updates

Major Releases	5.4	5.4.1										
	5.3	5.3.1	5.3.2	5.3.3								
	5.2	5.2.1	5.2.2	5.2.3	5.2.4	5.2.5	5.2.6					
	5.1	5.1.1	5.1.2	5.1.3	5.1.4	5.1.5						
	5.0	5.0.1	5.0.2	5.0.3	5.0.4	5.0.5	5.0.6	5.0.7	5.0.8	5.0.9		
	4.9	4.9.1	4.9.2	4.9.3	4.9.4	4.9.5	4.9.6	4.9.7	4.9.8	4.9.9	4.9.10	...
Minor Releases												

# WordPress Core: Automatic updates

Major Releases	5.4	5.4.1									
	5.3	5.3.1	5.3.2	5.3.3							
	5.2	5.2.1	5.2.2	5.2.3	5.2.4	5.2.5	5.2.6				
	5.1	5.1.1	5.1.2	5.1.3	5.1.4	5.1.5					
	5.0	5.0.1	5.0.2	5.0.3	5.0.4	5.0.5	5.0.6	5.0.7	5.0.8	5.0.9	
	4.9	4.9.1	4.9.2	4.9.3	4.9.4	4.9.5	4.9.6	4.9.7	4.9.8	4.9.9	4.9.10
											...
Minor Releases											

# Who is hacking my website?

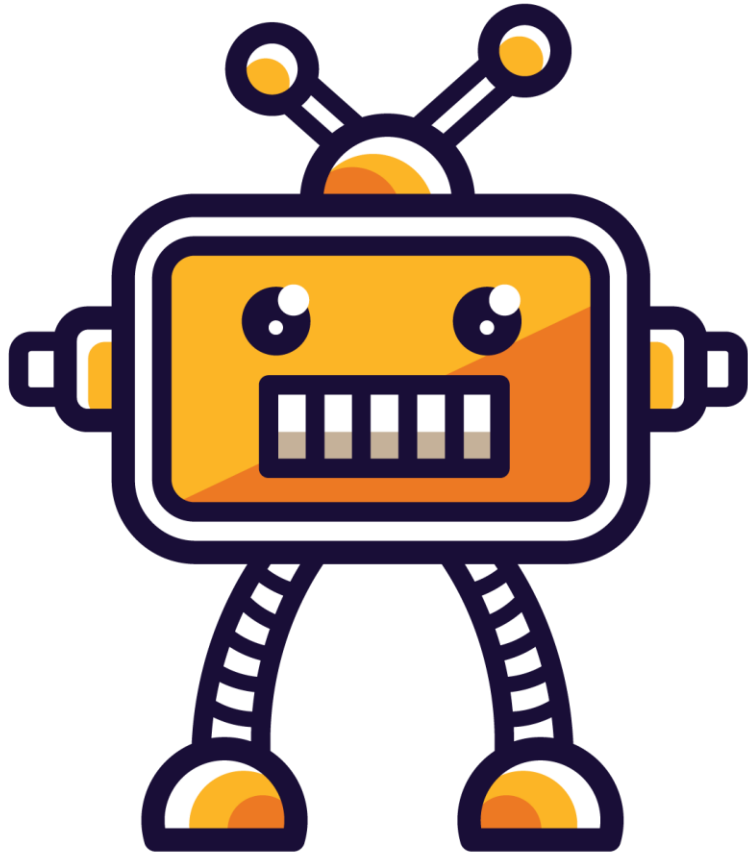
**Bots.**

It's not personal.

They don't hold a grudge.

But they'll hack you if you give them the chance.

Let's build a hypothetical bot, *TheArtisan*



“

I'm *TheArtisan*.

Bleep blop blorp.

”

# Instructions for our bot

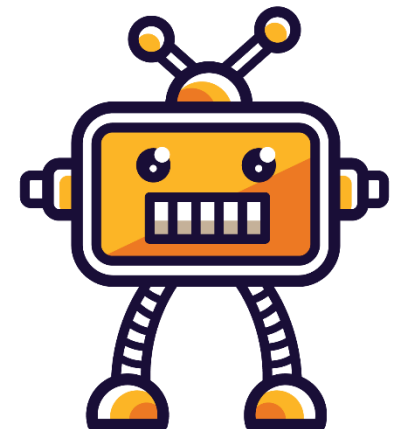
T H E A R T I S A N

# 1.



Try to import  
options with  
Easy WP SMTP  
plugin

If successful, embed:  
Email spam script.  
SEO Spam backlinks.  
Backdoor.



Easy WP SMTP <= 1.3.9 - Unauth

+

←

→

↺

https://wpvulndb.com/vulnerabilities/9237


☆

🔒

📁

👤

⋮



WordPress Plugins Themes API Submit Login Register

SEARCH

# Easy WP SMTP <= 1.3.9 - Unauthenticated Arbitrary wp\_options Import

Description

The changelog for easy-wp-smtp detailed that they "fixed potential vulnerability in import\export settings." in 1.3.9.1 of the plugin (SVN changeset 2052058). This was released on 17th March 2019.

It appears that an unauthenticated user can import arbitrary wp\_options by providing a PHP serialized array in `$_POST['swpsmtp_import_settings']`. This can be used to permit new user registrations and default their permissions to 'administrator'.

The vulnerability and fixes are detailed in the plugin SVN changelog: [https://plugins.trac.wordpress.org/changeset2old\\_path=%2Feasy-wp-smtp/](https://plugins.trac.wordpress.org/changeset2old_path=%2Feasy-wp-smtp/)



# Demonstration

E A S Y   W P   S M T P   O P T I O N S   I M P O R T

< = 1 . 3 . 9



# Instructions for our bot

THE ARTISAN

1.

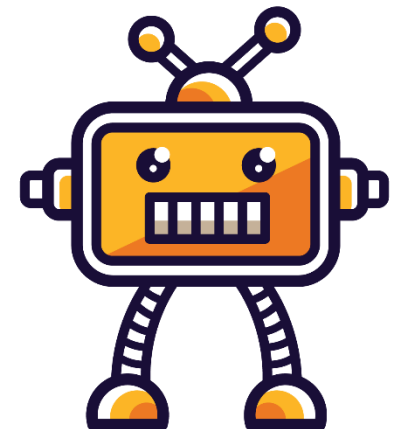
Try to import options with Easy WP SMTP plugin.

If successful, embed:  
Email spam script.  
SEO Spam backlinks.  
Backdoor.

2.

Next, try to exploit old Duplicator action to create new admin user.

If successful, embed malicious scripts.



Duplicator 1.3.24 & 1.3.26 - Unauth

+

←

→

↺

https://wpvulndb.com/vulnerabilities/10078


☆

🔒

📁

👤

⋮



[WordPress](#) [Plugins](#) [Themes](#) [API](#) [Submit](#) [Login](#) [Register](#)

SEARCH

# Duplicator 1.3.24 & 1.3.26 - Unauthenticated Arbitrary File Download

Description

The issue is being actively exploited, and allows attackers to download arbitrary files, such as the wp-config.php file.

According to the vendor, the vulnerability was only in two versions v1.3.24 and v1.3.26, the vulnerability wasn't present in versions 1.3.22 and before.

Proof of Concept

```
http://www.example.com/wp-admin/admin-ajax.php?action=duplicator_download&file=../wp-config.php
```



# Demonstration

D U P L I C A T O R   F I L E   D O W N L O A D

1 . 3 . 2 4   A N D   1 . 3 . 2 6

# Instructions for our bot

T H E   A R T I S A N

1.

Try to import options with Easy WP SMTP plugin.

2.

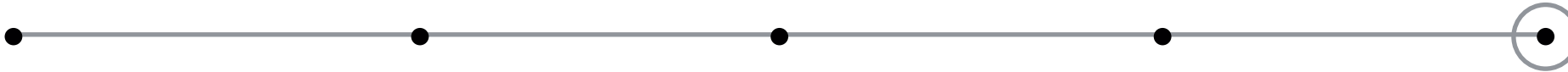
If successful, embed:  
Email spam script.  
SEO Spam backlinks.  
Backdoor.

Next, try to exploit old Duplicator action to create new admin user.

If successful, embed malicious scripts.

3.

Move on to the next website and start again.



# Instructions for our bot

THE ARTISAN

1.

Try to import options with Easy WP SMTP plugin.

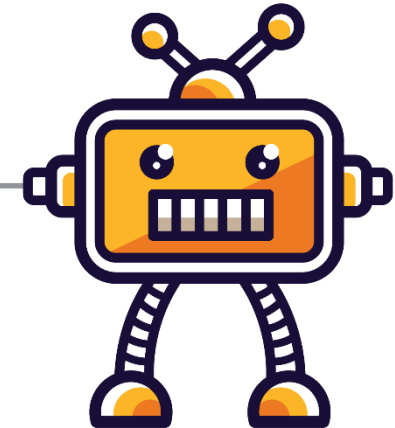
If successful, embed:  
Email spam script.  
SEO Spam backlinks.  
Backdoor.

2.

Next, try to exploit old Duplicator action to create new admin user.

If successful, embed malicious scripts.

Bots never rest



# So... should I enable automatic updates?

Well, maybe. It depends.

Here are some things to consider.

- ✓ Purpose of website
- ✓ Criticality of website
- ✓ Type of plugin
- ✓ QA resources of plugin author
- ✓ Your QA resources
- ✓ Who will resolve errors?

WordPress Plugins < Essence — WordPress

essence.lab/wp-admin/plugins.php

Essence

New WPForms

Howdy, essence

Dashboard

Posts

Media

Pages

Comments

WPForms

Genesis

Appearance

Plugins 1

Installed Plugins

Add New

Plugin Editor

Users

Plugins

Add New

All (4) | Active (3) | Inactive (1) | Update Available (1) | Must-Use (1) | Auto-updates Disabled (4)

Search installed plugins...

Bulk actions Apply 4 items

Plugin	Description	Automatic Updates
<input type="checkbox"/> Akismet Anti-Spam <a href="#">Activate</a>   <a href="#">Delete</a>	Used by millions, Akismet is quite possibly the best way in the world to <b>protect your blog from spam</b> . It keeps your site protected even while you sleep. To get started: activate the Akismet plugin and then go to your Akismet Settings page to set up your API key.  Version 4.1.6   By <a href="#">Automattic</a>   <a href="#">View details</a>	<a href="#">Enable auto-updates</a>
<input type="checkbox"/> Atomic Blocks - Gutenberg Blocks Collection <a href="#">Deactivate</a>	A beautiful collection of handy Gutenberg blocks to help you get started with the new WordPress editor.  Version 2.8.5   By <a href="#">atomicblocks</a>   <a href="#">View details</a>	<a href="#">Enable auto-updates</a>
<input type="checkbox"/> Duplicator	Migrate and backup a copy of your WordPress	<a href="#">Enable auto-updates</a>

Manage Themes < Genesis — Wo

+

← → ↻

genesis.lab/wp-admin/themes.php?theme=twentynineteen

☆ 👤 ⋮

WordPress

Genesis

1

0

+

New

WPForms

Howdy, genesis 👤

WordPress

WPForms

Genesis

Appearance

Themes

Customize

Widgets

Menus

Theme Editor

Plugins 1

Users

Tools

Settings

Atomic Blocks

Collapse menu

<

>

×

WordPress


Twenty Nineteen — The WordPress default theme for 2019

[Home](#) [About](#) [Blog](#) [Contact](#)

—

Welcome

Digital strategy for unique small businesses



Twenty Nineteen

Version: 1.7

By [the WordPress team](#)

Enable auto-updates

Our 2019 default theme is designed to show off the power of the block editor. It features custom styles for all the default blocks, and is built so that what you see in the editor looks like what you'll see on your website. Twenty Nineteen is designed to be adaptable to a wide range of websites, whether you're running a photo blog, launching a new

Activate

Live Preview

Delete

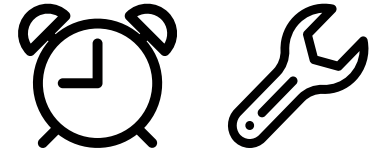


# Some best practices

- ✓ Make a backup of your website.  
And know how to restore it!
- ✓ Update WordPress core first.
- ✓ Use a child theme
- ✓ Update plugins and themes one at a time

Consider the 5-minute tune up...

# 5-Minute Website Tune-Up



- Google for your website.
- Click around the website before logging in.
- Check SSL Certificate
- Log in and check for updates.
- Update core (then verify)
- Update plugins and themes individually (verify after each update)



# Updating PHP

- PHP Compatibility Checker plugin
- Make a backup
- Request PHP upgrade from your hosting provider
- Test and verify
- If there is an issue, make sure you roll back the PHP upgrade *before* restoring your backup.

```
apt update && apt upgrade php*
```

# Updating PHP – Advanced method

```
apt install software-properties-common  
add-apt-repository ppa:ondrej/php  
apt update
```

Add repository for  
Advanced Packaging Tool

```
apt install php7.4
```

Install latest major release

```
apt install php7.4-extension_name
```

Install extensions

```
a2dismod php7.0  
a2enmod php7.4
```

Disable previous version  
and enable latest version.

# OK, let's review

Updates in WordPress Core (minor updates by default)

## Plugin and Theme updates

- Think about enabling automatic updates
- 5-Minute Website Tune-Up

## PHP Updates

- Contact your host

*apt update && apt upgrade php\**



# Questions?

Nick Wolfe



[ncwwolfe@gmail.com](mailto:ncwwolfe@gmail.com)



[github.com/wolfesq](https://github.com/wolfesq)