

Dan Wiseman

WordPress Security Basics



Web Wise
M E D I A

webwisemedиа.co.uk

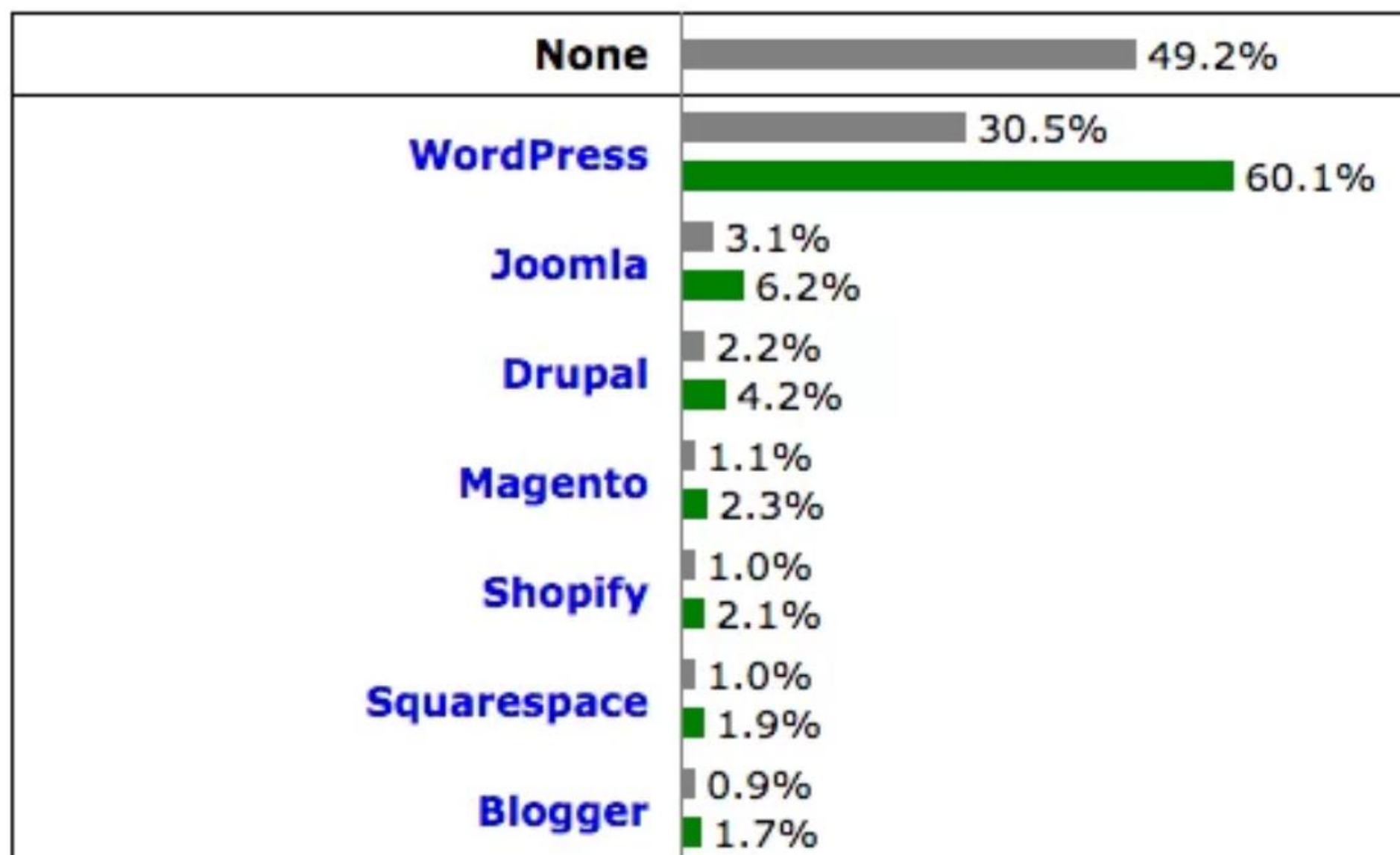
Outline

- Who is this for?
- Who am I
- Statistics
- Past experiences
- WordPress security basics



Who is this for?







The World's Worst Website

Gratuitous use of frames is a common mistake of web designers.

Many browsers do not support frames. They disrupt the flow of the website and can be difficult to anticipate where a page may appear when a link is clicked.

If you must use frames, use the tag `<base target="_blank">` between `<head>` and `</head>` to assure links will open in a new window.

Check out these links to websites whose opinions about frames is self evident:

[The "I Hate Frames" Frames Page](#)

[Another I Hate Frames Page](#)

[The International I Hate Frames Club](#)

Welcome To My Website!

Welcome to the World's Worst Website!

This web was designed to graphically demonstrate the most common mistakes made by new Web Page designers.

Where am I and where are the links to other pages?

An easy to use navigation structure is essential to any well designed website! Important information should never be more than 2 clicks away.



As you can see, this text is difficult to read. There needs to more contrast between the background color and the text color. [Here's another example](#) of a poor choice of a background/ text color and size.

Keep your backgrounds simple. White or light colors usually work best. Your background should not compete with the content of the page for the users attention. If you would like to use a background picture, select a picture that uses muted colors or format your picture as a watermark. Select text colors which will contrast well with the background picture.



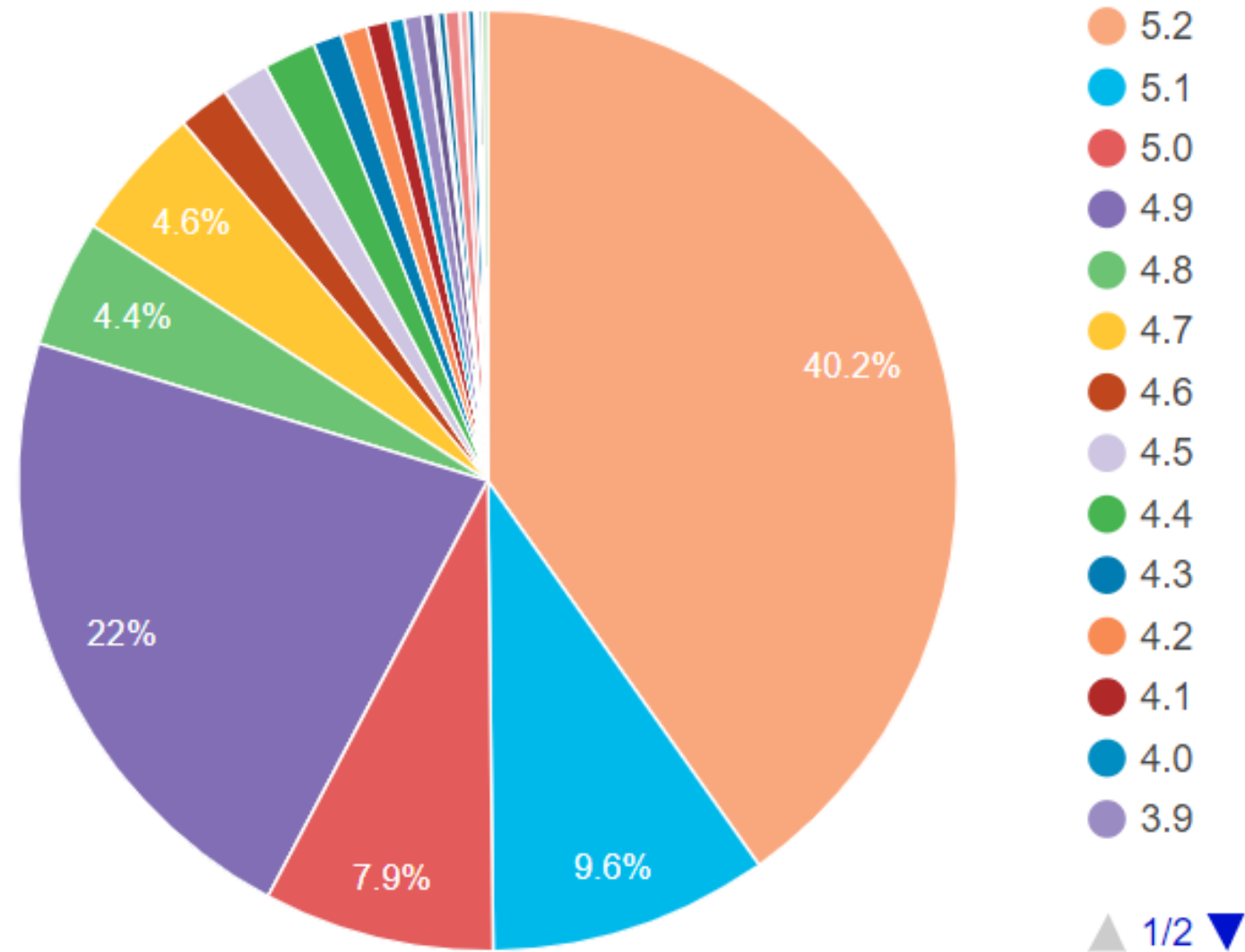
Constantly running animations can be distracting when used





Updating WordPress

WordPress Version



Panama Papers Leak in 2016,
which affected 2.6TB of data,
11.5million documents, and 4.8
million emails. The cause?...

**A website that wasn't running
the latest version of the 'Slider
Revolution plugin!'**

The world's most powerful WordPress Builder

with **ADVANCED ANIMATIONS**

Creating rich, dynamic content for web pages has never been easier.

 [Learn How](#)



WCBox – Woocommerce Plugin is help to display a list of products on WordPress Sidebar using Top Rated Products, Recent Products,Best Selling Products, ...

 Niloy Sarker

 60+ active installations

 Tested with 4.6.15



A simple and responsive content slider and slideshow plug-in for jQuery with features like touch and CSS3 transitions.

 Arthur Araújo

 300+ active installations


 Tested with 4.5.13



SWS responsive slider

★★★★★ (2)

SWS responsive slider plugin, is quite possibly the best way to show uploaded images in responsive slider. You can create as many responsive sliders a ...

 Technoscore

 Fewer than 10 active installations  Tested with 4.7.14



Device Mockups

★★★★★ (8)

Show your work in high resolution, responsive device mockups using only shortcodes.

 Justin Peacock

 4,000+ active installations

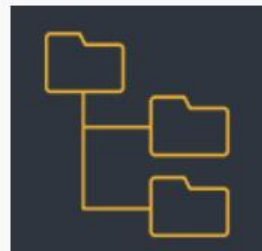
 Tested with 4.8.10



Slider Matches Results

☆☆☆☆☆ (0)

Allows you to create specific sliders for your sports team (Football, Handball ...).




Category Views by Webline

★★★★★ (1)

A Simple plugin allow you to upload category image and those displayed in front end with diff. display options.



WCBox – Woocommerce Plugin is help to display a list of products on WordPress Sidebar using Top Rated Products, Recent Products,Best Selling Products, ...

 Niloy Sarker

 60+ active installations

 Tested with 4.6.15



A simple and responsive content slider and slideshow plug-in for jQuery with features like touch and CSS3 transitions.

 Arthur Araújo

 300+ active installations


 Tested with 4.5.13




SWS responsive slider

★★★★★ (2)

SWS responsive slider plugin, is quite possibly the best way to show uploaded images in responsive slider. You can create as many responsive sliders a ...

 Technoscore

 Fewer than 10 active installations

 Tested with 4.7.14



Device Mockups

★★★★★ (8)

Show your work in high resolution, responsive device mockups using only shortcodes.

 Justin Peacock

 4,000+ active installations

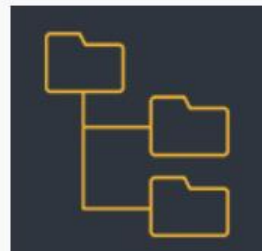
 Tested with 4.8.10



Slider Matches Results

☆☆☆☆☆ (0)

Allows you to create specific sliders for your sports team (Football, Handball ...).



Category Views by Webline

★★★★★ (1)

A Simple plugin allow you to upload category image and those displayed in front end with diff. display options.



WCBox – Woocommerce Plugin is help to display a list of products on WordPress Sidebar using Top Rated Products, Recent Products,Best Selling Products, ...

 Niloy Sarker

 60+ active installations

 Tested with 4.6.15



A simple and responsive content slider and slideshow plug-in for jQuery with features like touch and CSS3 transitions.

 Arthur Araújo

 300+ active installations


 Tested with 4.5.13




SWS responsive slider

★★★★★ (2)

SWS responsive slider plugin, is quite possibly the best way to show uploaded images in responsive slider. You can create as many responsive sliders a ...

 Technoscore

 Fewer than 10 active installations

 Tested with 4.7.14



Device Mockups

★★★★★ (8)

Show your work in high resolution, responsive device mockups using only shortcodes.

 Justin Peacock

 4,000+ active installations

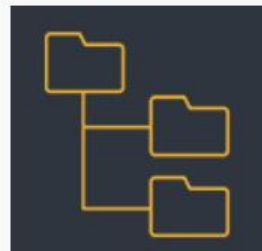
 Tested with 4.8.10



Slider Matches Results

☆☆☆☆☆ (0)

Allows you to create specific sliders for your sports team (Football, Handball ...).



Category Views by Webline

★★★★★ (1)

A Simple plugin allow you to upload category image and those displayed in front end with diff. display options.

[Products](#)[Solutions](#)[Resources](#)[For Developers](#)[For Enterprise](#)[Pricing](#)[Support](#) | [Sales: +44 20 3514 6970](#) | [English](#) ▶[Log In](#)[Sign Up](#)[Under Attack?](#)

Cloud Web Application Firewall

Cloudflare's enterprise-class web application firewall (WAF) protects your Internet property from common vulnerabilities like SQL injection attacks, cross-site scripting, and cross-site forgery requests with no changes to your existing infrastructure.

[Sign Up](#)[Contact Sales](#)

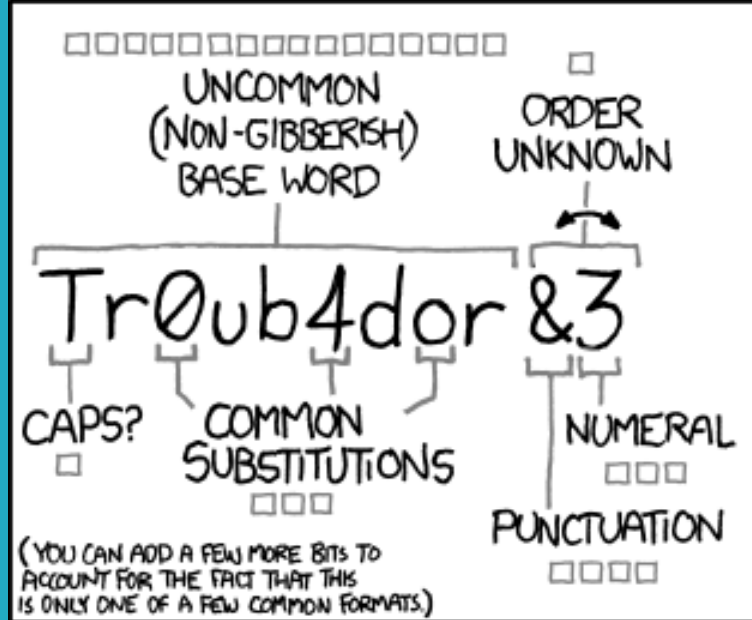
444,528,000
WAF rules triggered in the last day

WAF Triggers Map

Passwords, Passwords,
Passwords...

“81% of attacks are based on insecure or stolen passwords, being the main tactic used.

Source: <https://www.pandasecurity.com>



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

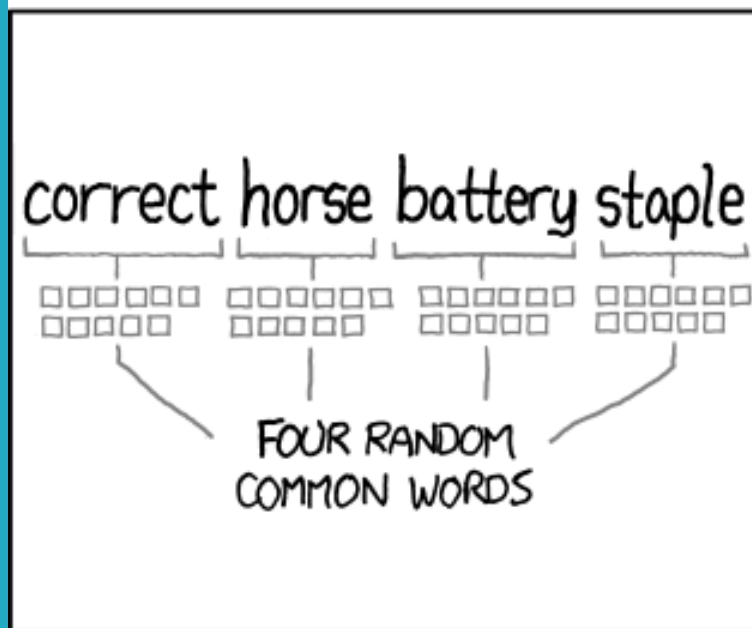
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

**“Top usernames being attacked:
admin, Admin, administrator,
test, root.”**

Source: <https://wpsmackdown.com>

How well do you know your
web developer?

What about *your* users?

Limit Login Attempts

“If you can protect yourself against plugin vulnerabilities and brute force attacks, you are accounting for over 70% of the security problem.”

Source: <https://www.wordfence.com>

Hosting

“41% were hacked through a security vulnerability on their hosting platform.”

Source: wpwhitesecurity.com



ReviewSignal

Shared	VPS	Dedicated	Reseller	Cloud	WordPress
Basic Hosting for most websites.	Partial Servers with full access.	Full Servers all to yourself.	Host Clients sell hosting.	Virtualize and Scale everything.	High Performance WordPress hosting.
<h2>WordPress Hosting Reviews</h2> <p>Sorted by Rating</p> <h3>Top WordPress Hosting Companies</h3>					
1	PANTHEON REVIEWS ▾	<div><div></div><div></div><div></div><div></div><div></div></div> 85% Rating	Starting at \$25	visit site ➔	
2	FLYWHEEL REVIEWS ▾	<div><div></div><div></div><div></div><div></div><div></div></div> 84% Rating	Starting at \$25	visit site ➔	
3	WPENGINE REVIEWS ▾	<div><div></div><div></div><div></div><div></div><div></div></div> 77% Rating	Starting at \$29	visit site ➔	
4	CLOUDWAYS REVIEWS ▾	<div><div></div><div></div><div></div><div></div><div></div></div> 76% Rating	Starting at \$7	visit site ➔	
5	KNOWNHOST REVIEWS ▾	<div><div></div><div></div><div></div><div></div><div></div></div> 76% Rating	Starting at \$12.95	visit site ➔	
6	SITEGROUND REVIEWS ▾	<div><div></div><div></div><div></div><div></div><div></div></div> 73% Rating	Starting at \$14.95	visit site ➔	
7	LIQUIDWEB REVIEWS ▾	<div><div></div><div></div><div></div><div></div><div></div></div> 71% Rating	Starting at \$119	visit site ➔	
8	PAGELY REVIEWS ▾	<div><div></div><div></div><div></div><div></div><div></div></div> 70% Rating	Starting at \$99	visit site ➔	
9	WPXHOSTING REVIEWS ▾	<div><div></div><div></div><div></div><div></div><div></div></div> 68% Rating	Starting at \$29	visit site ➔	



“Over 36% of all WordPress sites are served over HTTPS.”

Source: <https://hostingtribunal.com>

Backups



UpdraftPlus



FTP



UpdraftPlus

UpdraftPlus WordPress Backup Plugin

By UpdraftPlus.Com, DavidAnderson

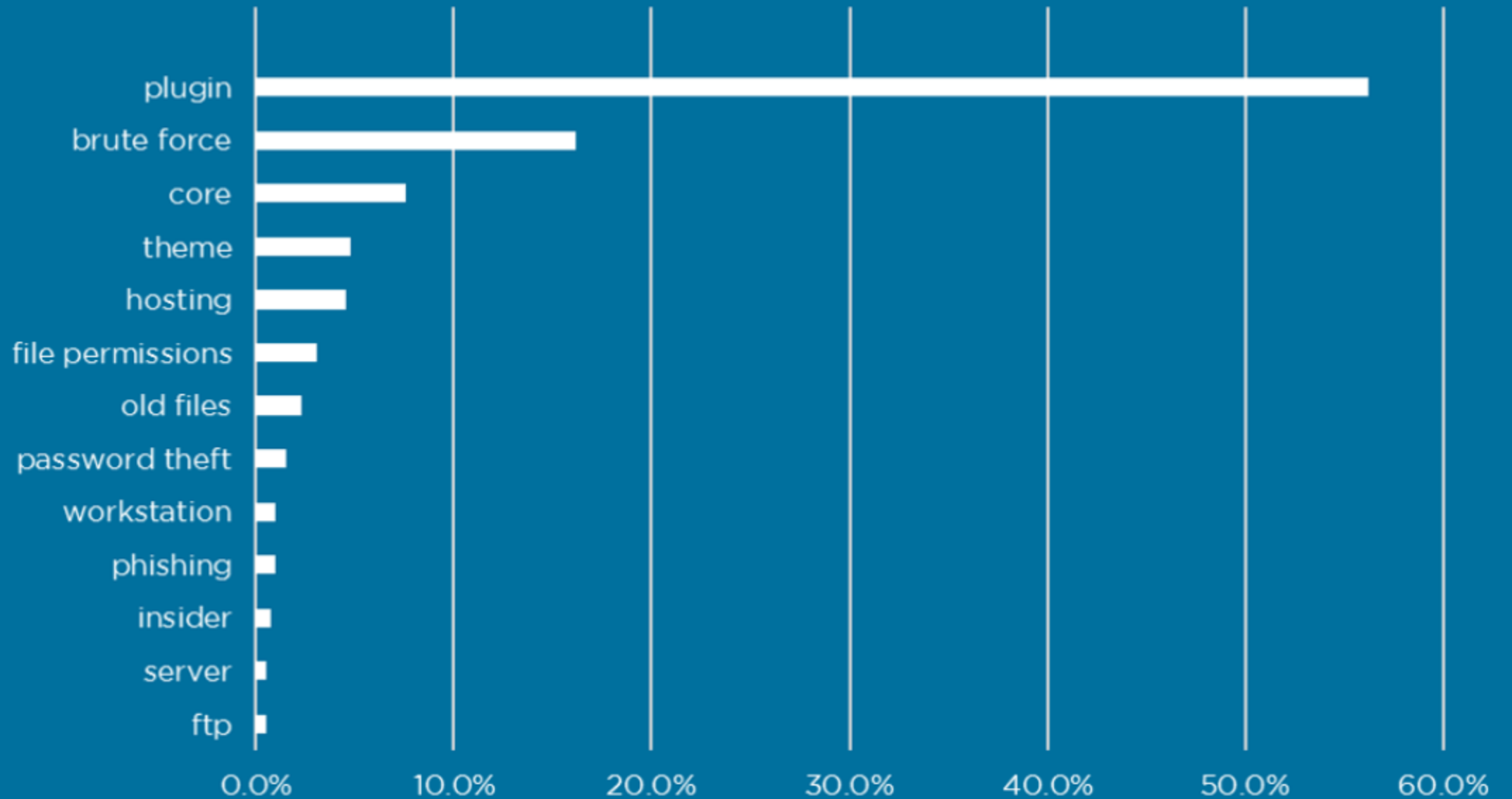
Download

Key Stats

- 41% of hacked WordPress were hacked through a security vulnerability on their hosting platform.
- 29% were hacked via a security issue in the WordPress Theme they were using.
- 22% were hacked via a security issue in the WordPress Plugins they were using.
- 8% were hacked because they had a weak password.

Source: <https://www.wpwhitesecurity.com>

How Hacked WordPress Sites Were Compromised



Summary

- Keep WordPress and Plugins up-to-date
- Don't use out of date plugins, abandoned plugins, untrustworthy plugins. Delete unused plugins from your site.
- Don't use an untrustworthy theme (hire a developer to build a bespoke one!)
- Get a good host and serve your site over HTTPS
- Get a strong, memorable password. Change your password regularly and educate your users about password security.



Web Wise
M E D I A

contact@webwise.media

Instagram:
[/web_wise_media](#)

Twitter:
[@Web_Wise_Dan](#)
[@webwisemedia_](#)

[webwisemedia.co.uk](#)

