So, then… Is WordPress Secure or Not?

By Nestor Angulo @pharar

WordFest.

DEFENSE & PROSECUTOR

Nestor Angulo

@pharar

- Very curious guy
  … more than a cat sometimes!
- Computer Science & Security Analyst

- Since 2015:
  Security Analyst @ **Sucuri**
- Since 2017:
  Advance Technical Support
  Managed SSL Analyst
  Developer in the WSS backend team
  @ **GoDaddy WebSecurity**

DEFENDANT

Trial Hearing Day:
27 July 2021

Is WordPress Secure or Not?

SECURITY FACTORS

What means Secure in a CMS scenario?

Protection of the Content & Information

No sharing info with 3rd Party companies

Hard in pentesting and HTTPS connection support

Roles and permissions management

Easy and frequent maintenance

Quick and effective support

The Chain of Trust

More windows and doors (plugins and themes) will make your fort harder to defend

Do you Trust in your software vendors? How much do YOU trust on them?

Trust is our weakest point: you delegate responsibility to a third party.

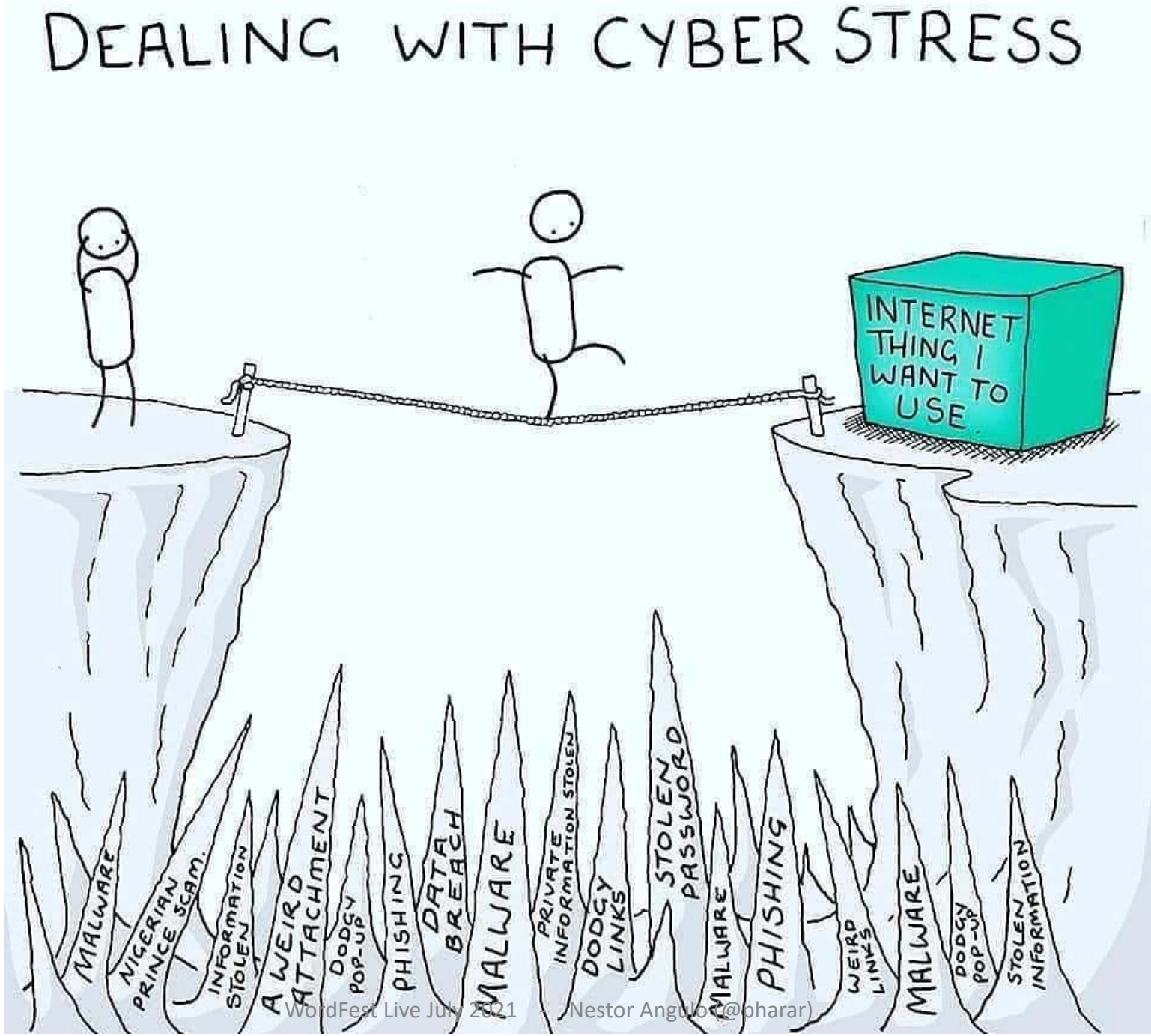
It is needed

Security: Simplified Layer Model

Layer	Protection

FACTS


There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked.
John Chambers
Chief Executive Officer of Cisco


DEALING WITH CYBER STRESS
INTERNET THING I WANT TO USE
MALWARE
NIGERIAN PRINCE SCAM.
INFORMATION STOLEN
A WEIRD ATTACHMENT
DODGY POP-UP
PHISHING
DATA BREACH
MALWARE
PRIVATE INFORMATION STOLEN
DODGY LINKS
STOLEN PASSWORD
MALWARE
PHISHING
WEIRD LINKS
MALWARE
DODGY POP-UP
STOLEN INFORMATION

FACTS

Site hacking **almost never** is client-oriented (98% of cases)

Almost always happens due to a **deficient monitoring / maintenance**

A **SSL** certificate **is not** an antihacking shield

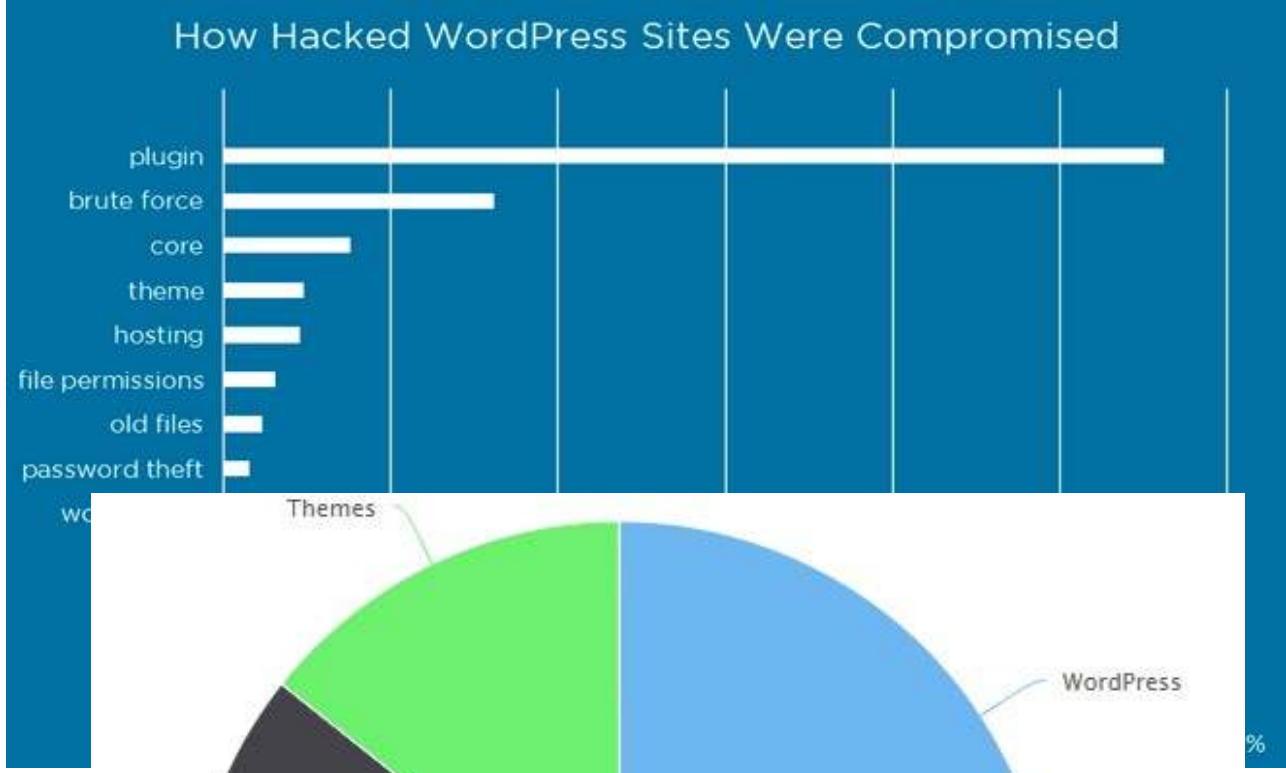
Patches & security updates appear almost always after hacking exploits

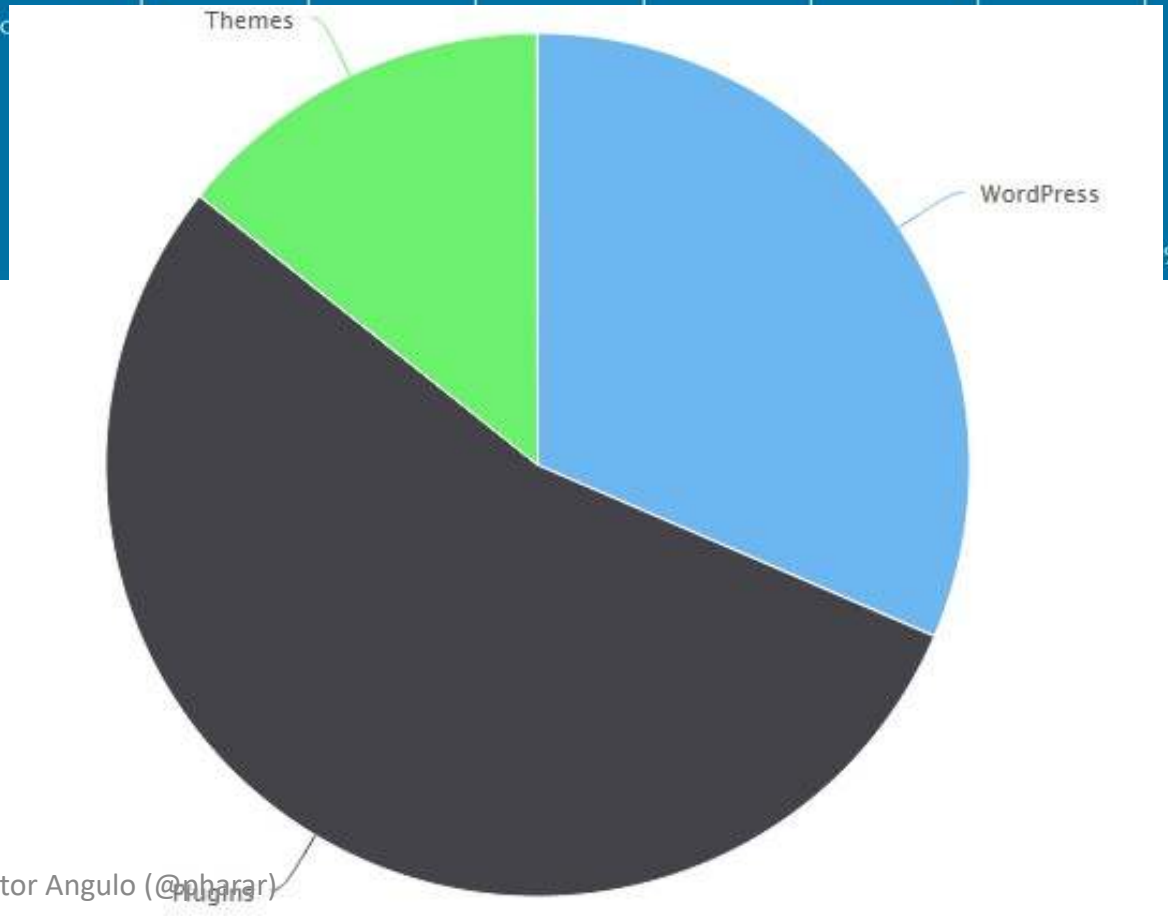
Errare Humanum Est (Human being fails)

Security **never is (nor will be)** 100% effective

The Chain of Trust

- Themes & plugins
- Embeded Code & content
- Gravatar, Google Fonts, emojis, etc.
- Analytics, Firewall, CDN, Hosting. Etc.





Plugin Name	Installations
Easy WP SMTP	400,000
Wp File Manager	500,000
Freemius Library (Multiple plugins are affected)	200,000
Newspaper and other old tagDiv Themes	100,000
WordPress GDPR Compliance	100,000
Social Warfare	70,000
WP Live Chat Support	60,000
Yuzo Related Post	60,000
WP-Piwik	60,000
Sticky Menu on Scroll, Sticky Header for Any Theme	60,000

Support and Maintenance 

- WordPress updates are frequent and there is a clear roadmap
- **Open Source,** anybody can fix and propose improves (millions of potential developers). Bazaar model.
- One of the biggest tech communities in the World.
- **WordPress community** is in charge of the support, it is similar to a forum and **multilanguage**.
- In some local communities (i.e. the Spanish one), all the support questions get answered within the same day usually.

Roles, permissions and HTTPS

WordPress has roles management and access control, even for its API

It can be customised and improved using plugins

Works smooth over HTTPS

Doesn’t force HTTPS by default, and you can’t manage it easily. A plugin is needed and sometimes some hand work is needed.

Information protection, privacy and sharing to 3rd party

By default, the sensitive information is encoded and protected.

By default, WordPress don’t share any information with 3rd party companies.

Strong passwords are not forced, nor 2FA. A plugin is needed here.

”Out of the box”, it doesn’t protect the privacy of your site in a strict way:

- Gravatar, emojis, WordPress, embedded content, etc.
- It doesn’t give native support to GDPR, cookies, CCPA, etc.

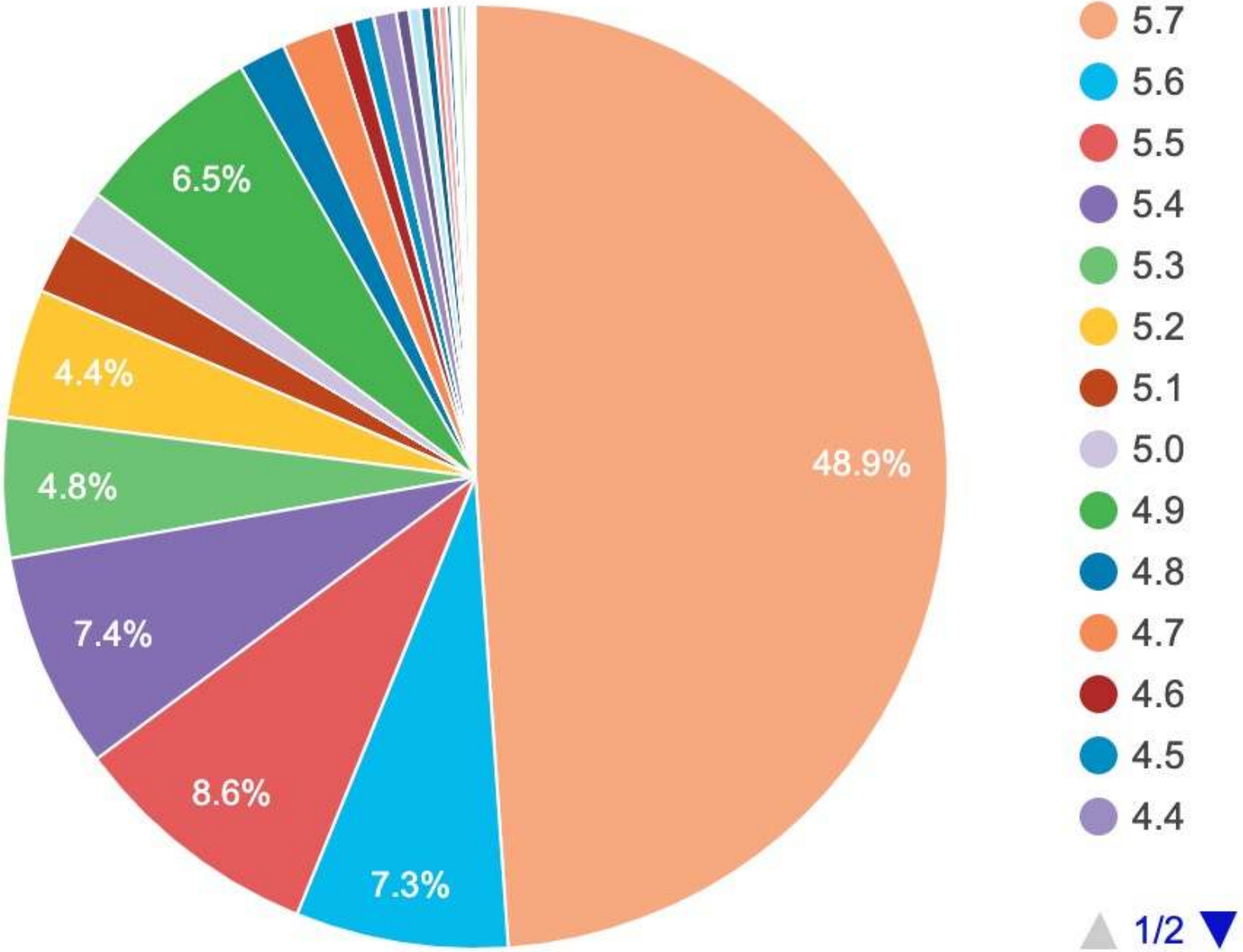
”Out of the box”, it doesn’t have any backup process nor audit tools.

More about WordPress security

wordpress.org/about/security

Updates

- Source:
WordPress version distribution at July 2021
– wordpress.org



How Frequently do you Install Security Patches for your clients'?

AUTOMATIC UPDATES ENABLED (208)

36.9%

AS SOON AS POSSIBLE (172)

30.5%

CLIENTS ARE RESPONSIBLE (72)

12.8%

WHENEVER I HAVE TIME (69)

12.2%

WHEN PROMPTED OR CLIENT REQUESTS (30

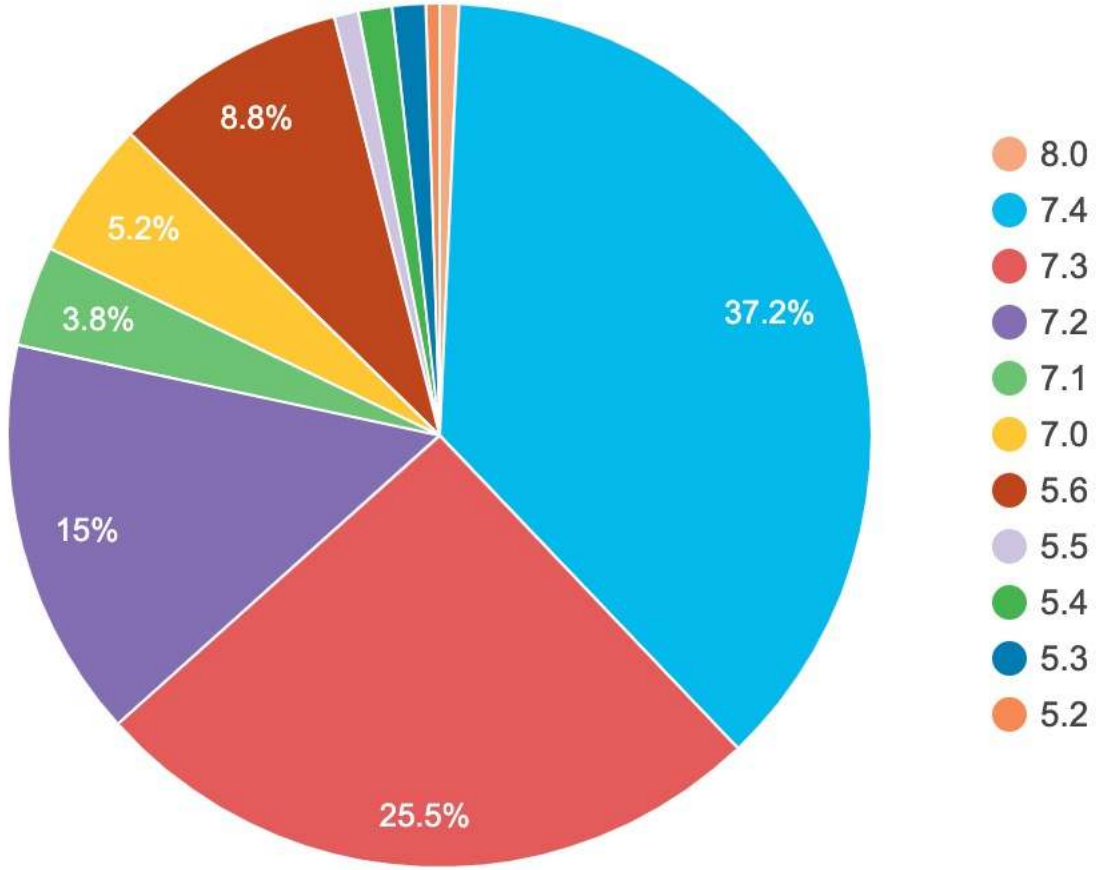
5.3%

I DON'T (13)

2.3%

PHP Versions

Sources:
Web Professional Security Survey 2019 (Sucuri.net)
PHP versions distribution July 2021 (wordpress.org)



VERDICT!

Is WordPress secure?

Is WordPress secure?

YES (with reservations)

At least, all it can be “out of the box”

So, what's the problem here?

It is EXTREMELY easy to create an INSECURE WordPress

Examples

Admin users named as “admin” and easy-to-remember passwords.

Install plugins from not official repositories or freemium or downloaded from “weird” sites

Not protecting your site connection using HTTPS and reliable SSL certificates

The Believer Risk

Believe	**that the perfect cheap hosting exists**
Believe	**that the security is for paranoids and/or “others” are in charge of it.**
Believe	**that your site or content is not interesting for any cybercriminal**

Thanks a lot!

QUESTIONS!!

WordFest.