So, then…
Is WordPress Secure or Not?

By Nestor Angulo @pharar

Stellar WP

✨ Stellar Spark Conference

Trial Hearing Day:
19th July 2024

Is WordPress Secure or Not?

DEFENSE & PROSECUTOR

Nestor Angulo

@pharar

- Very curious guy, coffee lover and digital nomad
- CISSP & Software Engineering Manager @ **Patchstack**

patchstack

- 2015 - 2023:
  Security Analyst @ **Sucuri**
  Advance Technical Support
  Managed SSL Analyst
  Developer in the WSS backend team
  @ **GoDaddy WebSecurity**

DEFENDANT

Trial Hearing Day:
19th July 2024

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

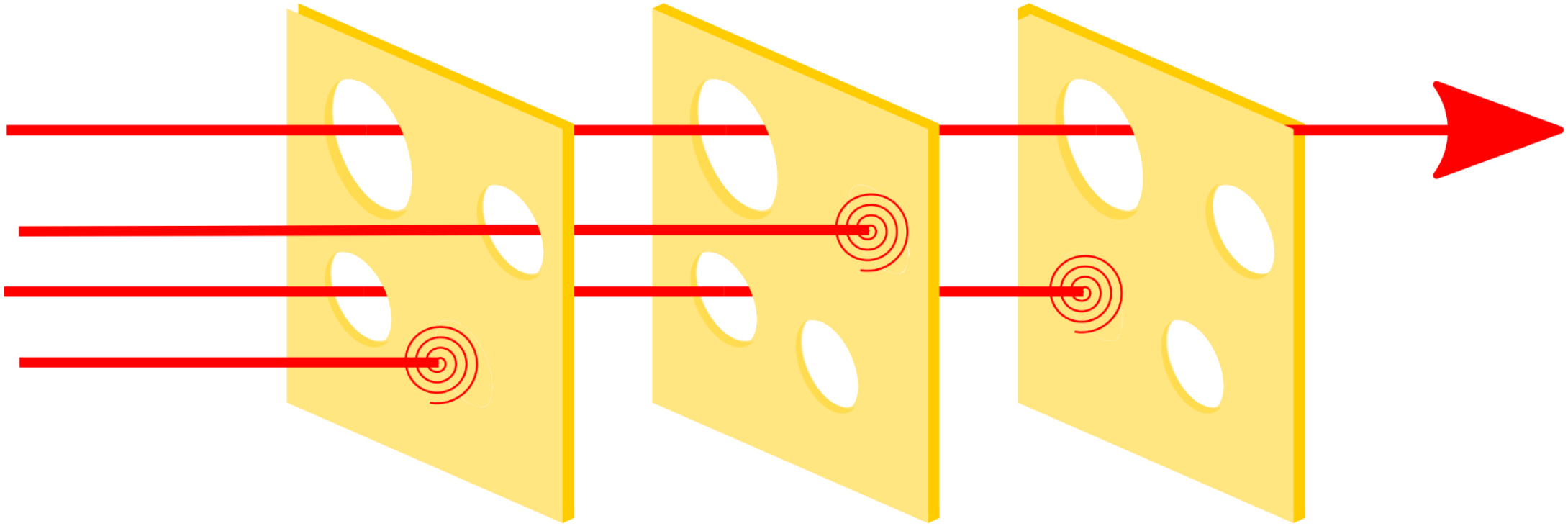
Rapid fix and Easy and frequent maintenance

Quick and effective support

Security: Sir

Swiss Cheese permeability model

- Defense-in-Depth
- No single intervention is sufficient to prevent the harm



FACTS

Security in WordPress

WORDPRESS CARES ABOUT SECURITY IN CORE

DELEGATES SECURITY IN PLUGINS, THEMES, HOSTING COMPANIES, SITE OWNERS/ADMINS, ETC.

The Chain of Trust

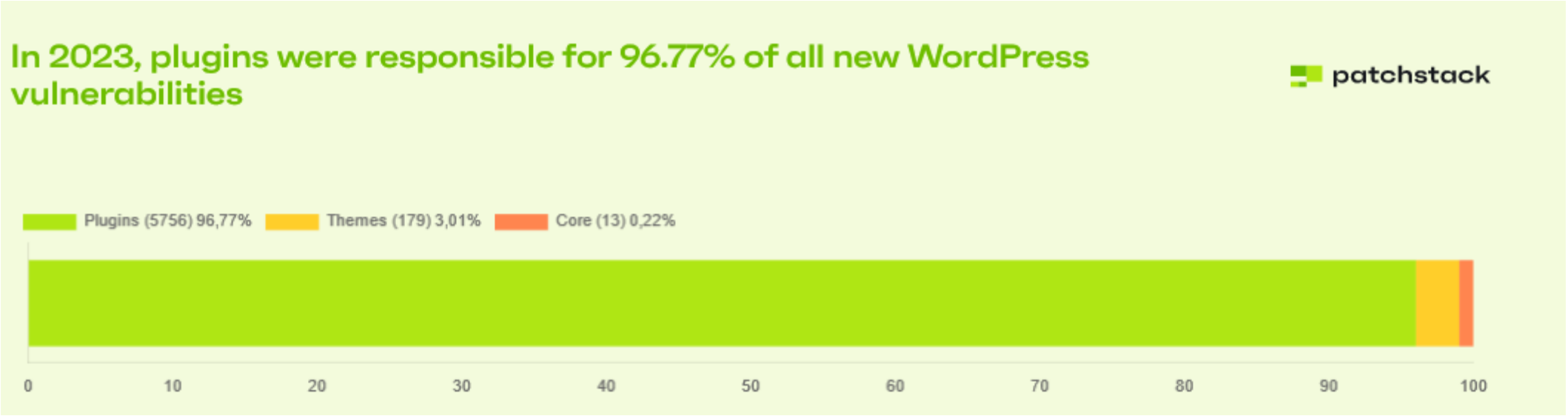
More windows and doors (plugins and themes) will make your fort harder to defend

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.

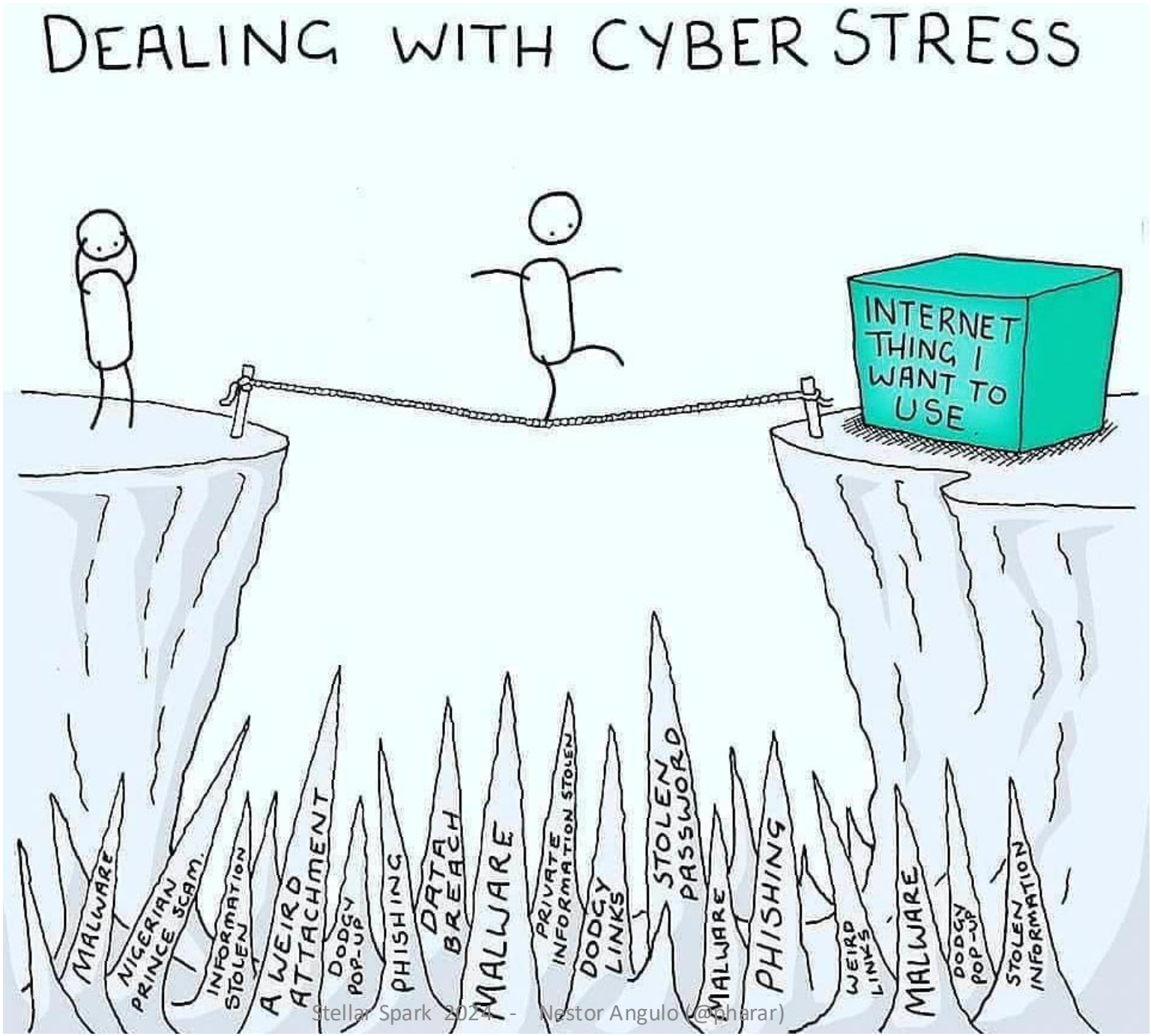
It is needed

The Chain of Trust



- Core, themes & plugins
- Embedded Code, comments & content of the site
- Gravatar, WordPress.org, Google Fonts, Youtube, emojis, etc.
- Analytics, Firewall, CDN, Hosting. Etc.


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

Most severe vulnerabilities found in popular plugins in 2023

patchstack

Component	Installs	Vulnerability	CVSS	Prereq.	Researcher
Essential Addons for Elementor	1,000,000	Privilege Escalation	9.8	Unauthenticated	Rafie Muhammad (Patchstack)
WP Fastest Cache	1,000,000	SQL Injection	9.3	Unauthenticated	Alex Sanford
Gravity Forms	940,000	PHP Object Injection	8.3	Unauthenticated	Rafie Muhammad (Patchstack)
Fusion Builder	900,000	SQL Injection	8.5	Subscriber	Rafie Muhammad (Patchstack)
Flatsome (Theme)	618,000	PHP Object Injection	8.3	Unauthenticated	Rafie Muhammad (Patchstack)
WP Statistics	600,000	SQL Injection	9.9	Subscriber	Rafie Muhammad (Patchstack)
Forminator	400,000	Arbitrary File Upload	9.8	Unauthenticated	mehmet
WPvivid Backup and Migration	300,000	Privilege Escalation	8.8	Subscriber	Nguyen Anh Tien
JetElements For Elementor	300,000	Broken Access Control	8.2	Unauthenticated	Rafie Muhammad (Patchstack)

How WordPress does in terms of security?

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

Rapid fix and Easy and frequent maintenance

Quick and effective support

Information protection, privacy and sharing to 3rd party

- ✅ By default, the sensitive information is encoded and protected.
- ✅ By default, WordPress doesn'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.org, Gfonts, 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.

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, and sometimes some handwork, is needed.

Support and Maintenance

- **WordPress updates are frequent** and there is a clear roadmap
- v6.6 introduced plugins rollback!
- **Open Source,** anybody can fix and propose improves (millions of potential developers). Bazaar model.
- **WordPress community (one of the biggest in the world)** is in charge of the support, it is similar to a forum and **multilanguage**.

Code quality and vulnerabilities

- ✅ Enforces code style
- ✅ Enforces tests
- ✅ Have a central point to report vulnerabilities
- ✅ WordPress core dedicated group
- ✅ WordPress plugins security dedicated group
- ✅ Committers by merits
- ❌ Compatibility backwards is higher priority, which causes some delays in vulnerabilities fixing.

Some Security features I'm missing

- ✕ Force a CAPTCHA field for every form in the site (To avoid Spam) and feature for banning users which try incorrect credentials repeatedly (To avoid Brute Force attacks)
- ✕ Audit tools to back trace every user action
- ✕ More information about abandoned/closed plugins
- ✕ Backups and HTTPS native support
- ✕ More security controls over plugins and themes

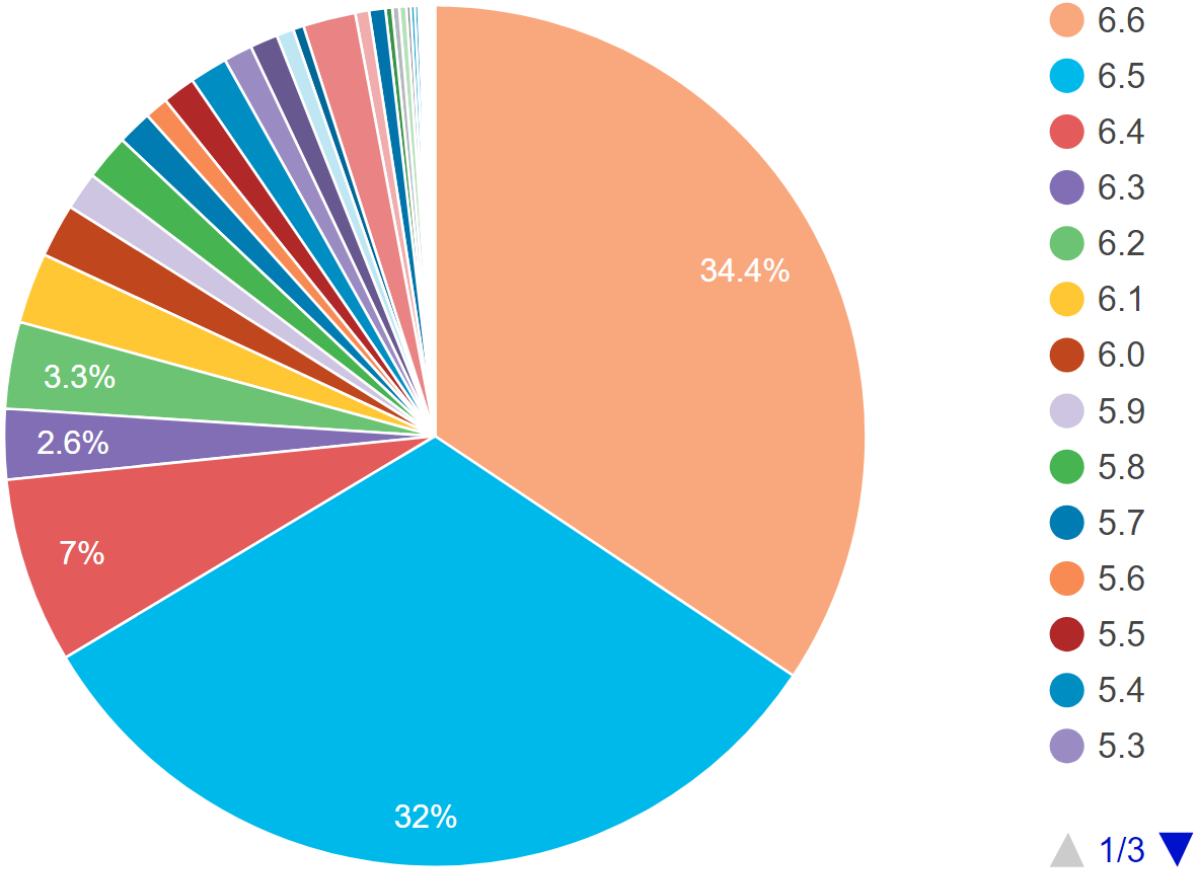
More about WordPress security

wordpress.org/about/security

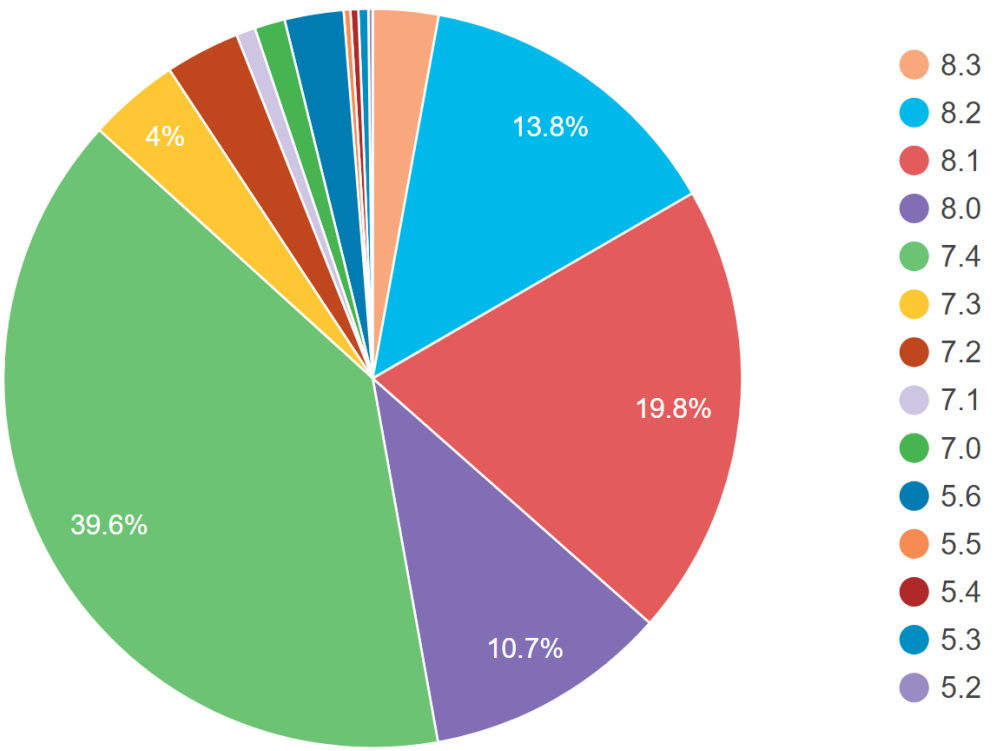
Open Website Alliance and the CRA

Updates

- Source:
WordPress version distribution at July 2024
– wordpress.org



- **PHP versions distribution** July 2024 (wordpress.org)



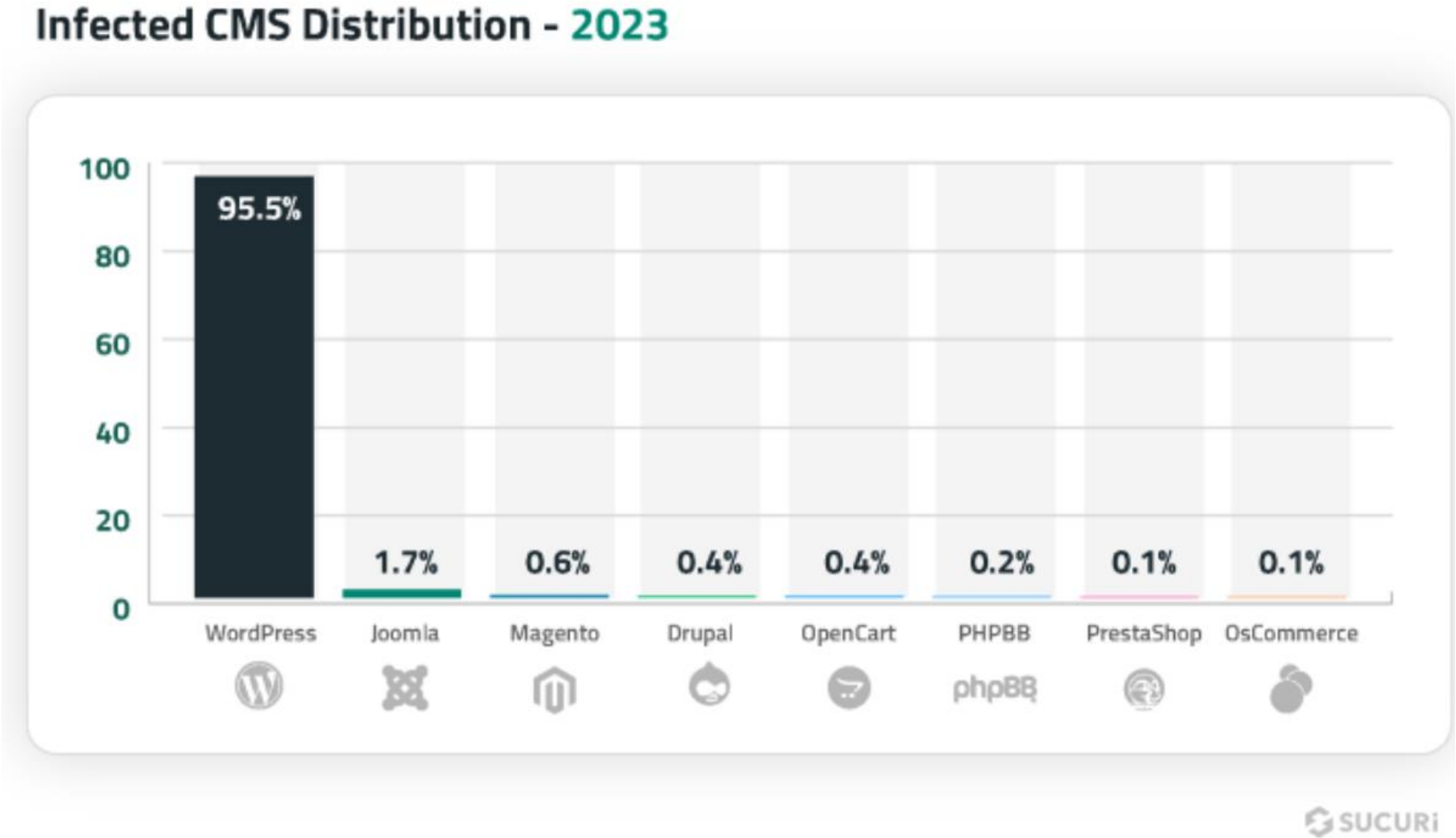
VERDICT!

Is WordPress secure?

Is WordPress secure?

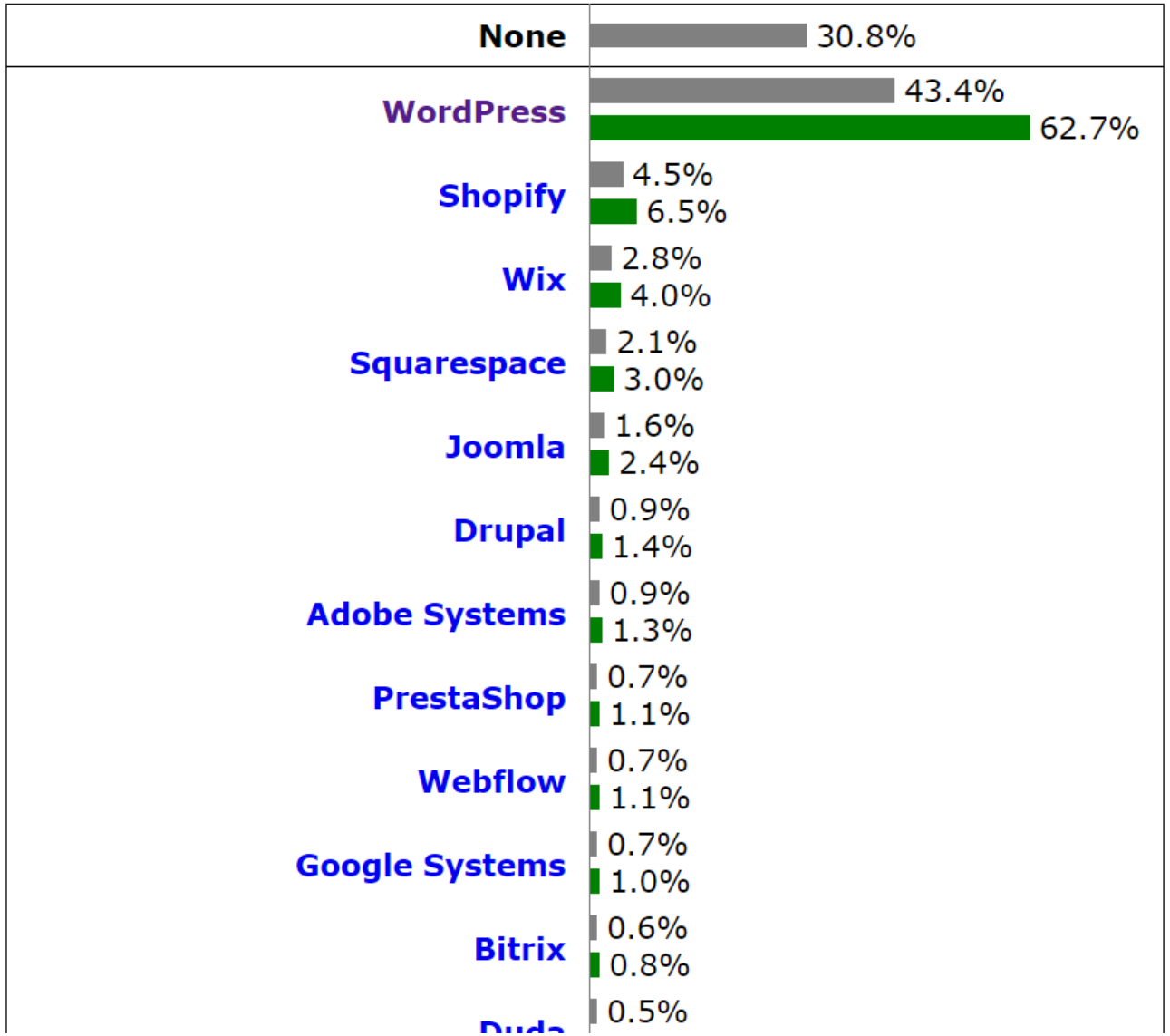
YES, if updated.

At least, all it can be “out of the box” (WordPress core)



2023 Hacked Website & Malware Threat Report from **Sucuri**.
https://sucuri.net/reports/2023-hacked-website-report/

How to read the diagram:
30.8% of the websites use none of the content management systems that we monitor.
WordPress is used by 43.4% of all the websites, that is a content management system market share of 62.7%.



W3Techs - https://w3techs.com/technologies/overview/content_management

So, what's the problem here?

It is **EXTREMELY easy** to create an **INSECURE** WordPress.

You will need to **TRUST in plugins**

Examples

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

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

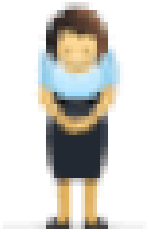
Not protecting your site connection using HTTPS and reliable SSL certificates

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**


Everybody needs a hacker

Thanks a lot!



QUESTIONS!!