Hardening Wordpress

Securify

A guide to stop or recover from a Pwn…

Part 1: General info

(What ?)

Part 1: General info

- Content Management System
- Open Source
- PHP & MySQL
- Structure:
- ***Core***
- ***Themes***
- ***Plugins***

Core + Themes + Plugins =

Core + Themes + Plugins =

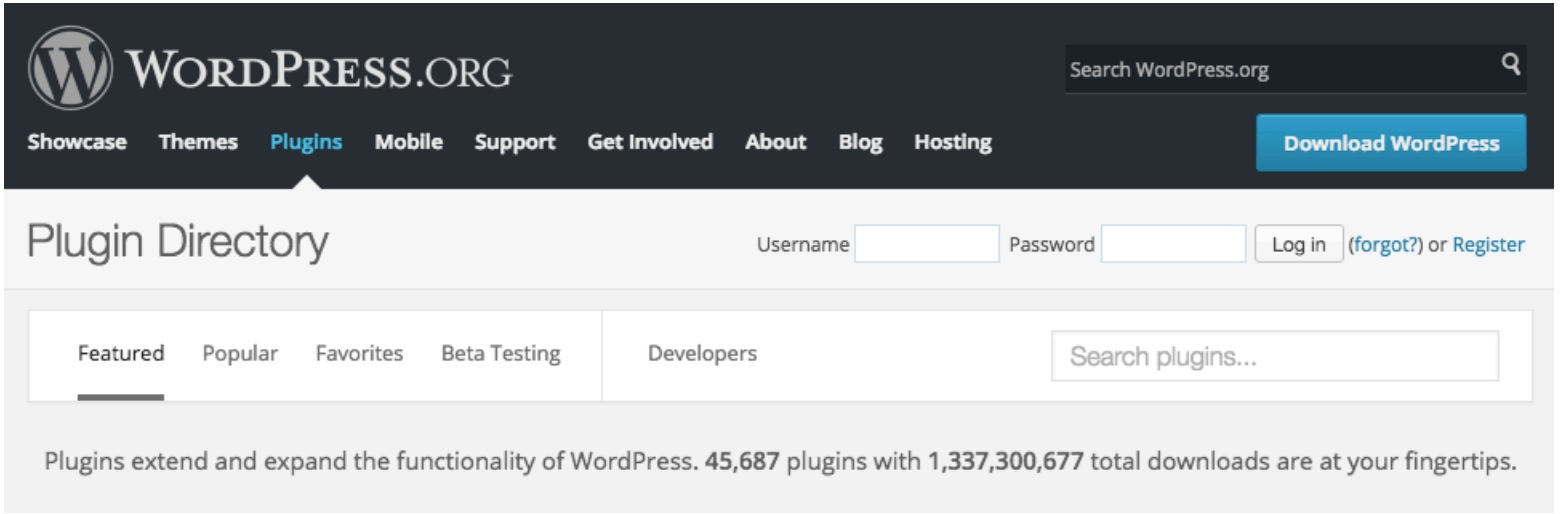
Core + Themes + Plugins =

Core + Themes + Plugins =

Minimum to work

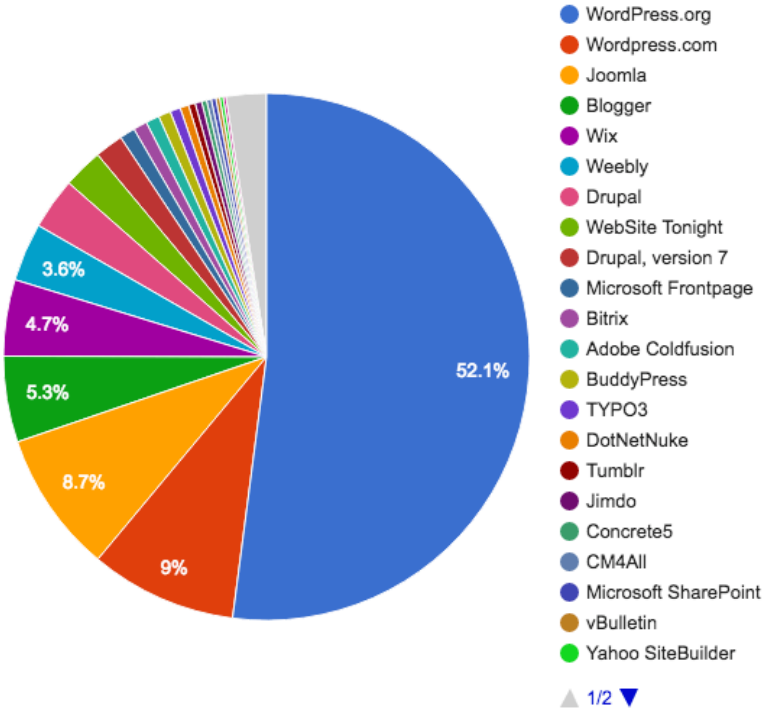
Extra functionality

45k+ Plugins!
~ 10k Themes



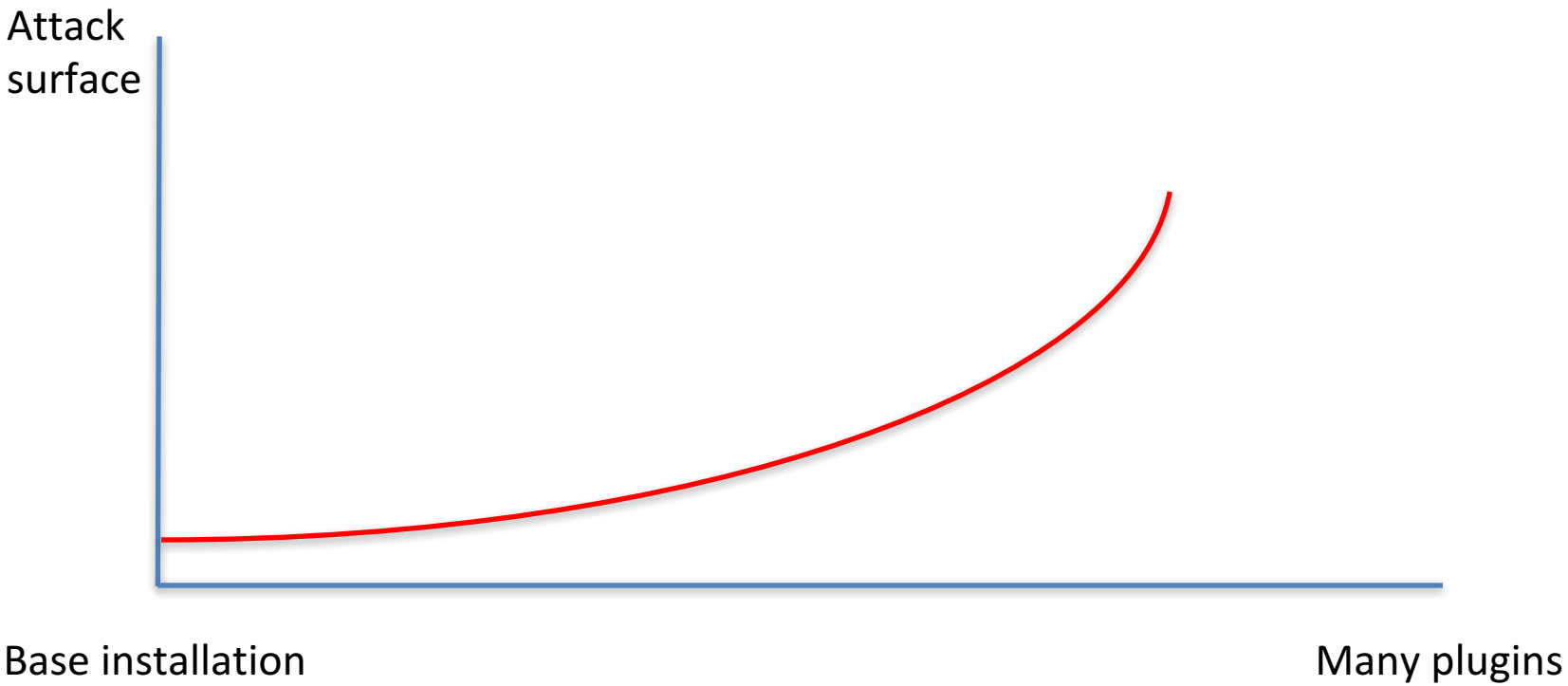
Wordpress marketshare

Alexa top 1M



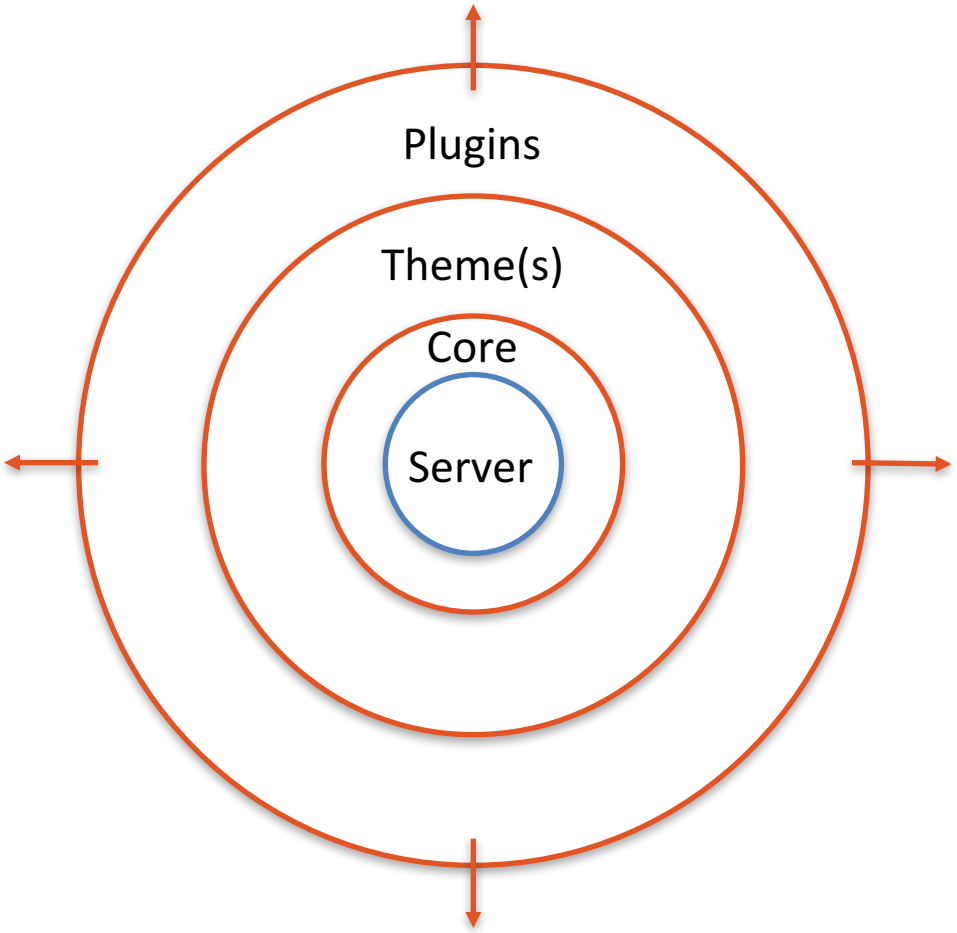
https://www.datanyze.com/market-share/cms/

Attack Surface



Part 2: Prevent a Pwn

(Be proactive)


Plugins
Theme(s)
Core
Server

Three ways of hosting Wordpress:

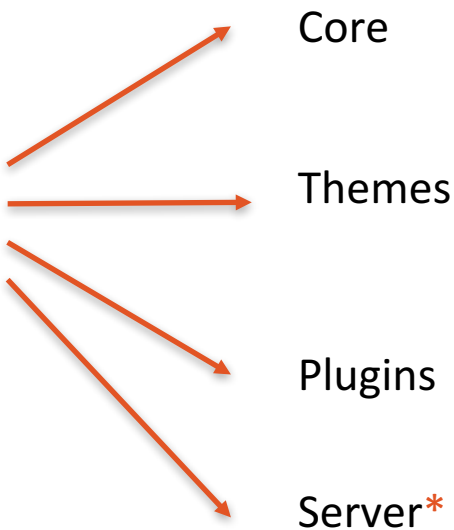
1. Shared Hosting Service
2. Managed (hybrid)
3. Self Hosting*

Hardening Wordpress

Security 101

Updates!

Updates everywhere…



Use **strong** passwords!

Avoid:

- Short passwords → Use at least 8 chars (or more…)
- Passwords containing known info like name, address, date of birth, pets etc…
- Common dictionary words
- Only numerical or alpha → Best mix it up
- …

Hardening Wordpress

Security 101

~~FTP~~ access → SFTP

- Encrypted password
- Encrypted data

Backups!

- Regularly
- Off server

Pro Tip:

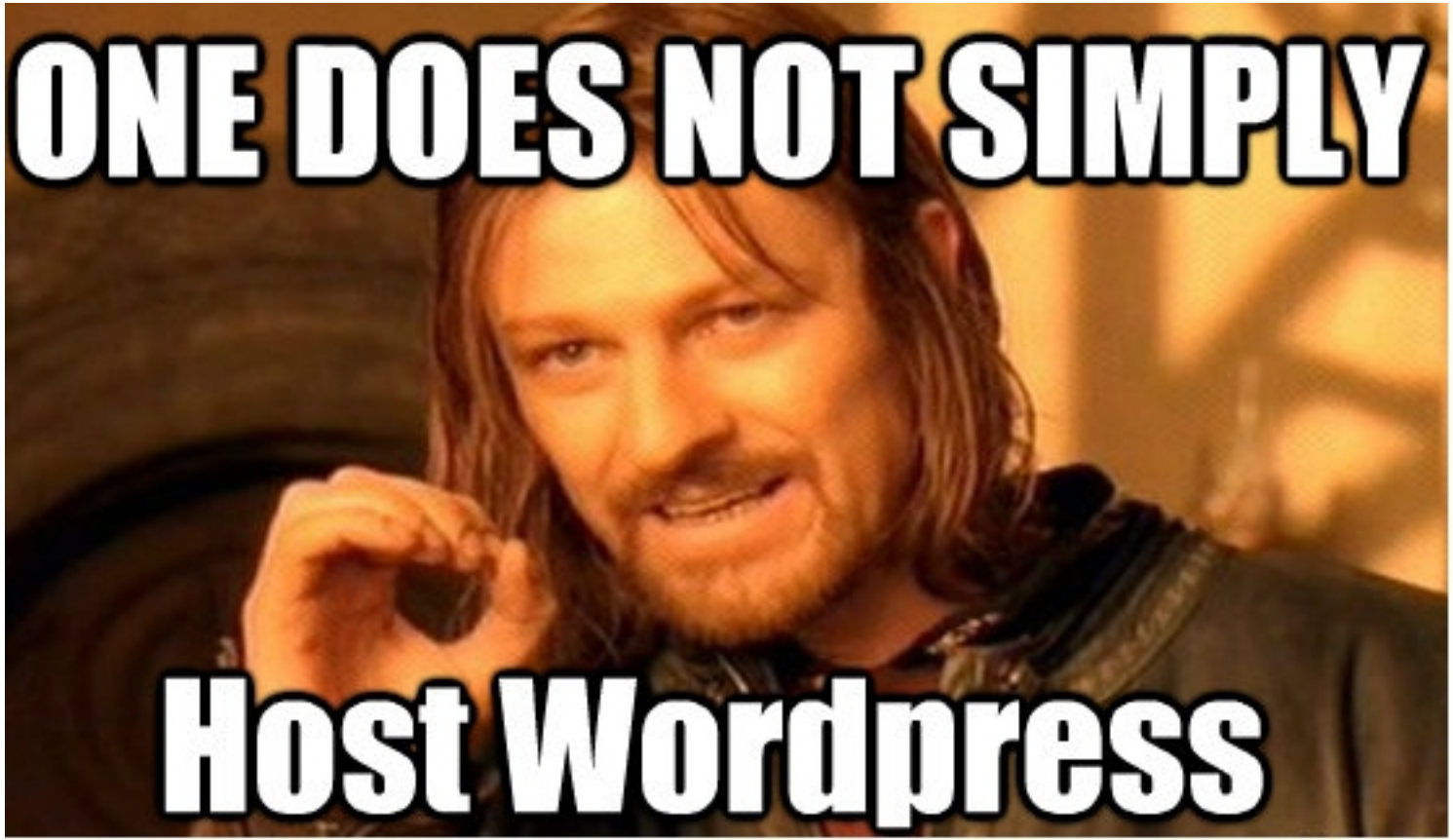
- Keep a copy of a clean installation + your base configuration as in day-0

Use Child themes when tweaking with appearance

Three ways of hosting Wordpress:

1. Shared Hosting Service
2. Managed (hybrid)
3. Self Hosting*

*


ONE DOES NOT SIMPLY
Host Wordpress

Hardening Wordpress

Server

Before starting with Wordpress hardening, make sure you are set with:

- Infrastructure
- Apache
- PHP
- MySQL

Then… Move on!

Fine tune file permissions

- Directories:
  755
- Files:
  644
- /wp-admin/ → All files must be writeable only by user account
- /wp-includes → All files must be writeable only by user account
- /wp-content → Must be writeable from user and web server

Restrict access to the admin panel

- Add a .htaccess file to wp-admin:

  Order Deny,Allow
  Deny from all
  Allow from 127.0.0.1

- Add server-side password protection (BasicAuth)
- Whitelist allowed IPs
- Enforce the administrator(s) to use VPN and/or SSH
- Delete (or change) the admin account
- Use different name than account login name

Secure wp-config.php

Move the file one directory above the Wordpress installation

- (site installed in web root → wp-config.php will be outside web root and internet)
- User and web server should have read permissions (400 or 440)
- Wordpress will automatically search one directory above if file not in web root
- You can add a .htaccess file with:

```
<files wp-config.php>
order allow,deny
deny from all
</files>
```

Disable directory listing or add blank index.php files

Now the directories are not browse-able
Main folders to protect:

- *wp-includes*
- *wp-content*
- *wp-content/plugins*
- *wp-content/themes*
- *wp-content/uploads*

Hardening Wordpress

Server

It’s all about what is exposed

Google dorks

- inurl:wp-config.txt
- Inurl:/wp-content/plugins/{vuln plugin name}

Part 3: I got Pwned!

(What now…?)

Recover from a Pwn

Step 1: Stay calm!

Then, move on…

Recover from a Pwn

If you don’t have a clean back up, take one NOW!

Recover from a Pwn

Analyze the damage

- Usually, a piece of malicious code is injected in JS files for spamming purposes
- https://sitecheck.sucuri.net - You can scan your site to see what is the damage

Recover from a Pwn

Install a fresh Wordpress installation and theme/plugins as well

- Make sure to have the wordpress downloaded from official source!

Recover from a Pwn

… Start over …

What if you had done Part 1 and Part 2 earlier…??

Thank you!