Almost everything that's wrong with WordPress 😄

Christian Leo-Pernold

@mazedlx

https://github.com/mazedlx

https://mazedlx.net

Agenda

State of WordPress 📊

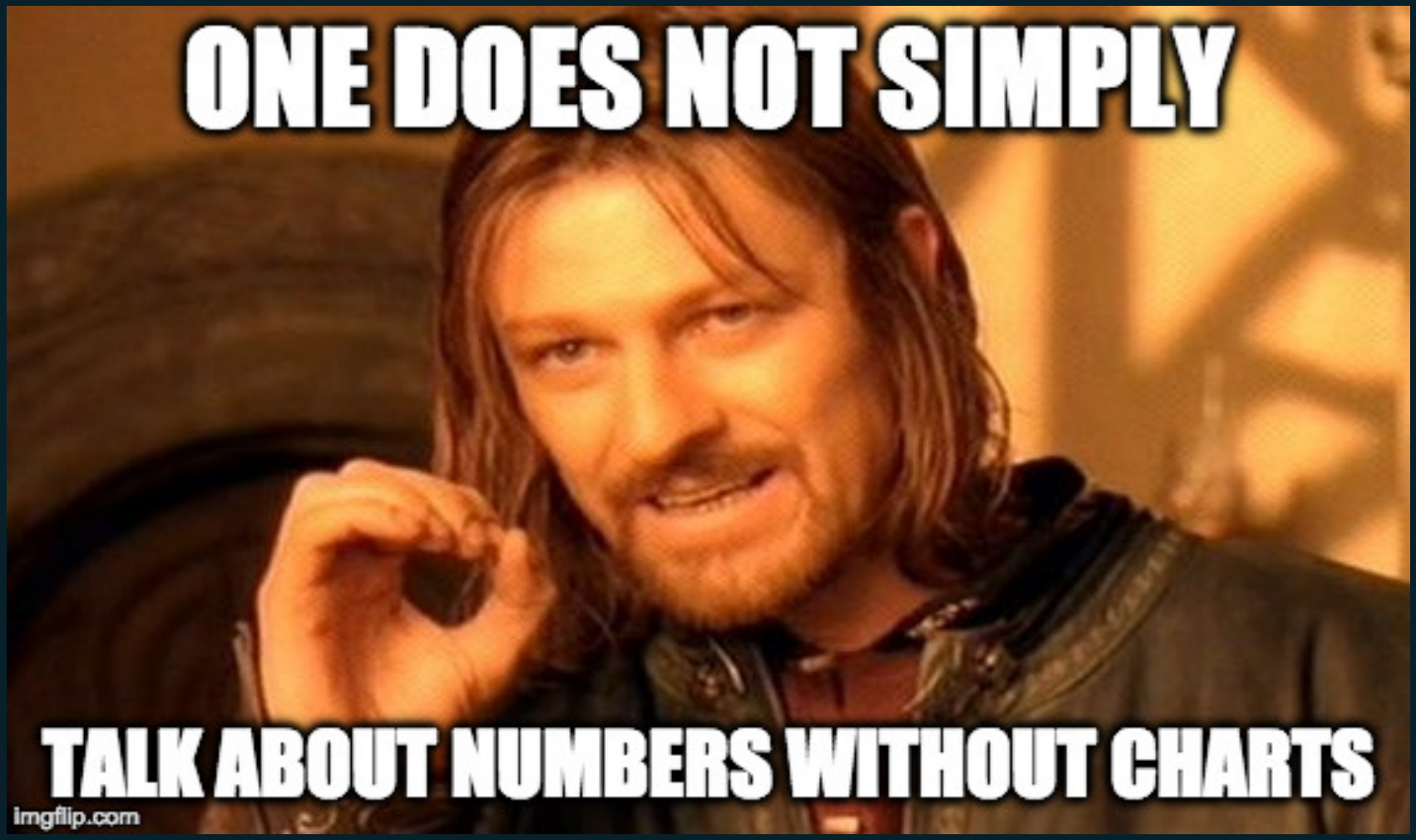
Developer’s POV 👩‍💻

Vulnerabilities 🔓

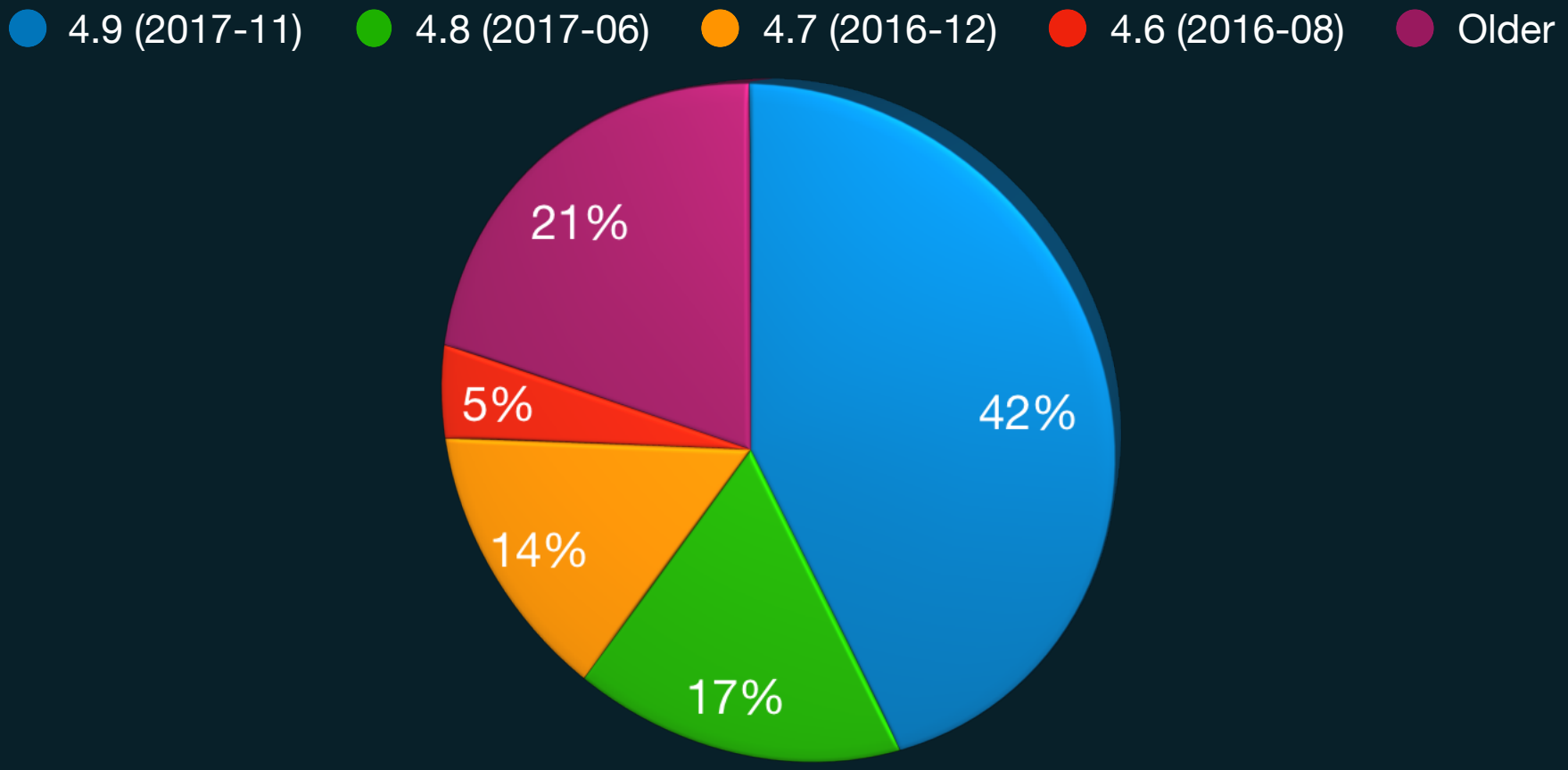
Conclusion 🏁

Lots of Memes 🤣

State of WordPress 📊

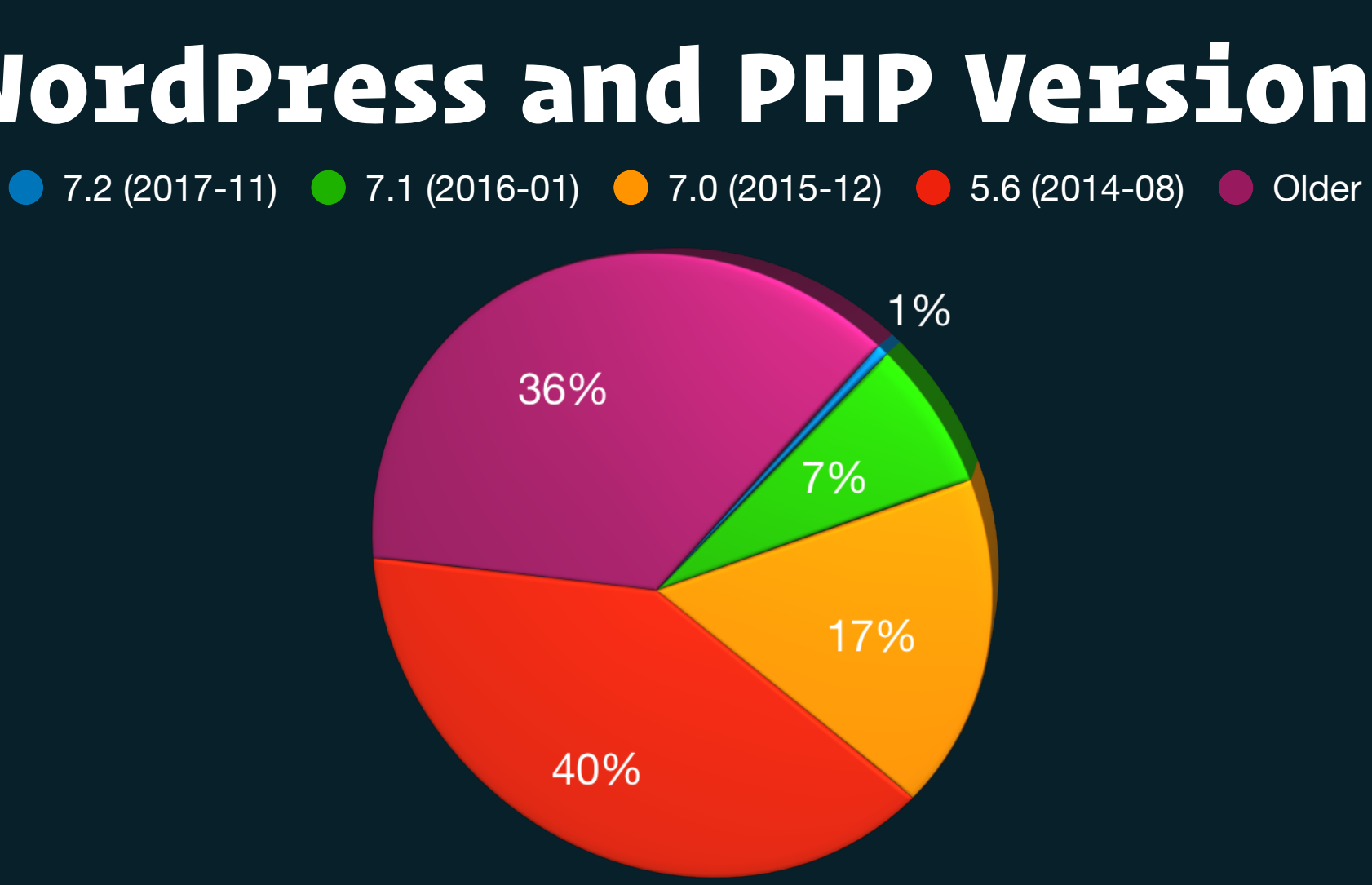

ONE DOES NOT SIMPLY
TALK ABOUT NUMBERS WITHOUT CHARTS
imgflip.com

WordPress Versions



Source: https://wordpress.org/about/stats

WordPress and PHP Versions



Source: https://wordpress.org/about/stats

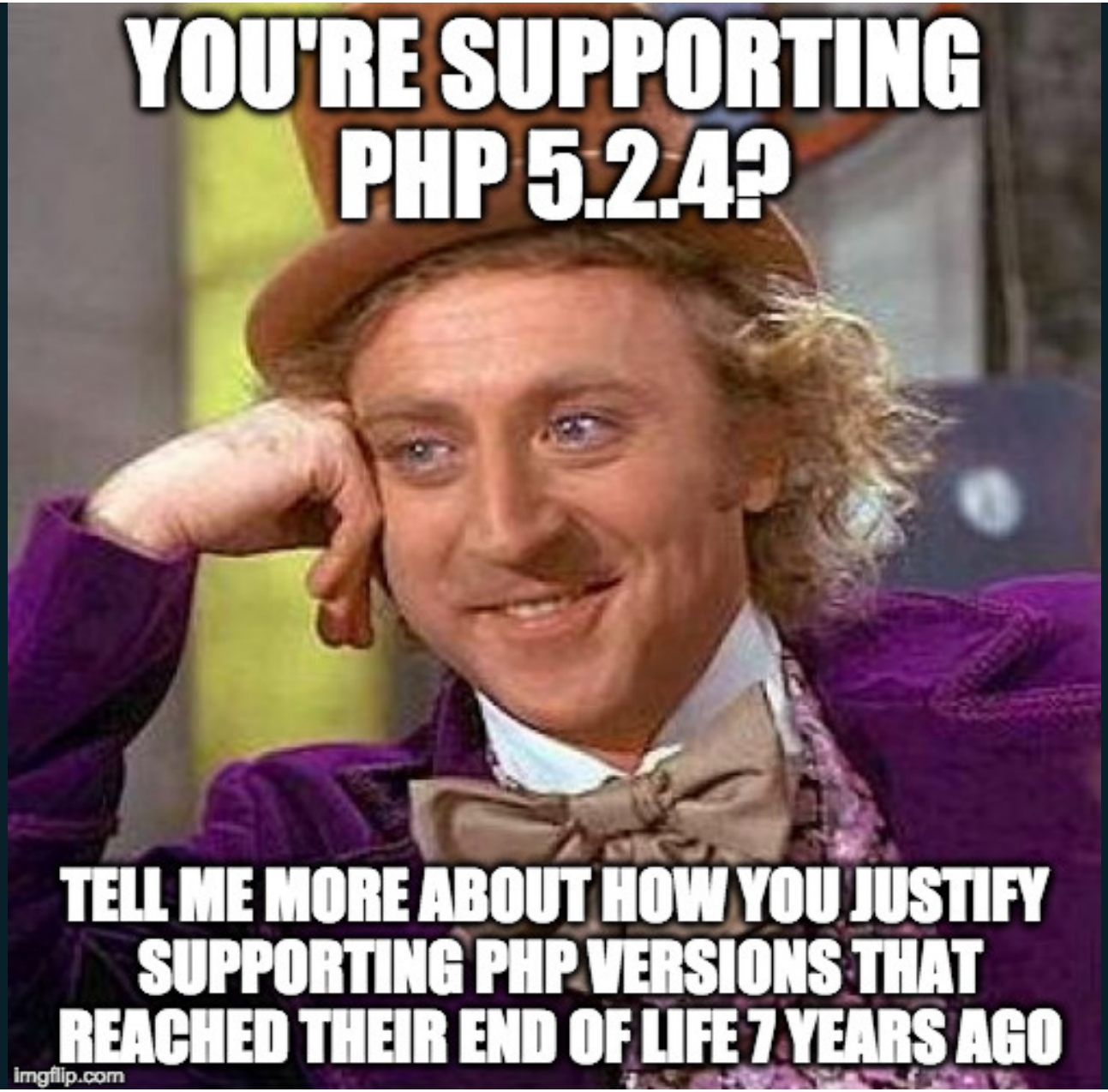
“

Why do we support older versions?

We strongly **recommend the latest versions** of PHP and MySQL, but we understand that this isn’t right for everyone, and that sometimes hosts can be slow or hesitant to upgrade their customers since upgrades to PHP and MySQL have historically broken applications.

Note: If you are in a legacy environment where you only have older PHP or MySQL versions, WordPress also works with PHP 5.2.4+ and MySQL 5.0+, but these versions have reached official End Of Life and as such **may expose your site to security vulnerabilities**

Source: https://wordpress.org/about/requirements/


YOU'RE SUPPORTING PHP 5.2.4?
TELL ME MORE ABOUT HOW YOU JUSTIFY SUPPORTING PHP VERSIONS THAT REACHED THEIR END OF LIFE 7 YEARS AGO
imgflip.com

More numbers

~ 29% market share (of CMS) 🔥

~ 50.000 Plugins 🔌

~ 60 translations 🇪🇸🇩🇪🇬🇧🇯🇵🇨🇳🇮🇹

~ 77.000.000 blogs 📝

~ 16.000.000 sites 💻

~ $50 developer hourly rate 😢

Source: https://w3techs.com, https://www.codeinwp.com and https://managewp.com

Well-known WordPress Users

Snoop Dogg 🎤

NY Times Blogs 📰

Forbes Blogs 📰

Vogue 📰

Bloomberg Professional 📰

BBC America 📺

TechCrunch 📰

GNOME 🚀

Mercedes-Benz 🚘

Playstation.Blog 🎮

Le Monde 📰

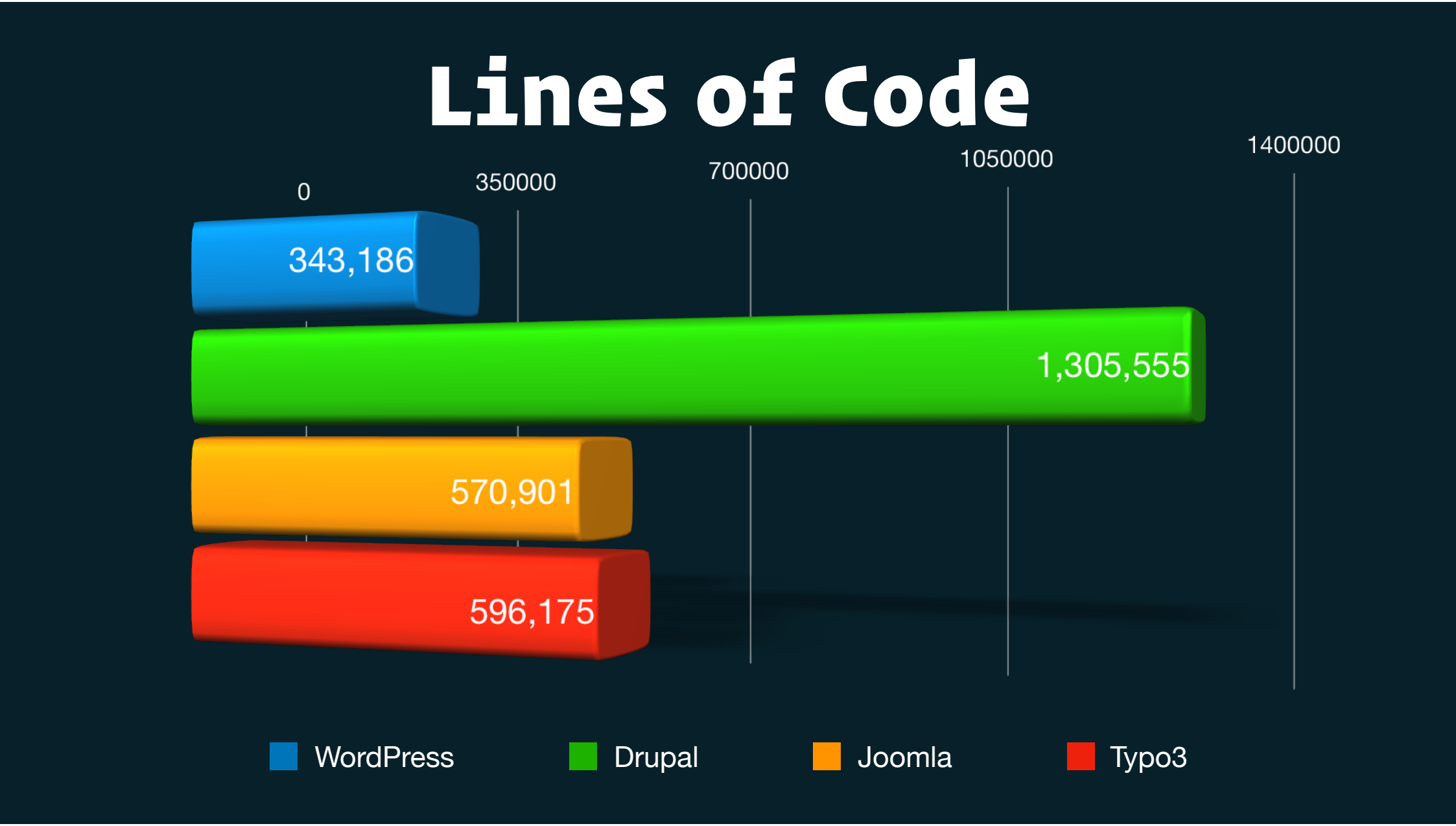
The Walt Disney Company 💼

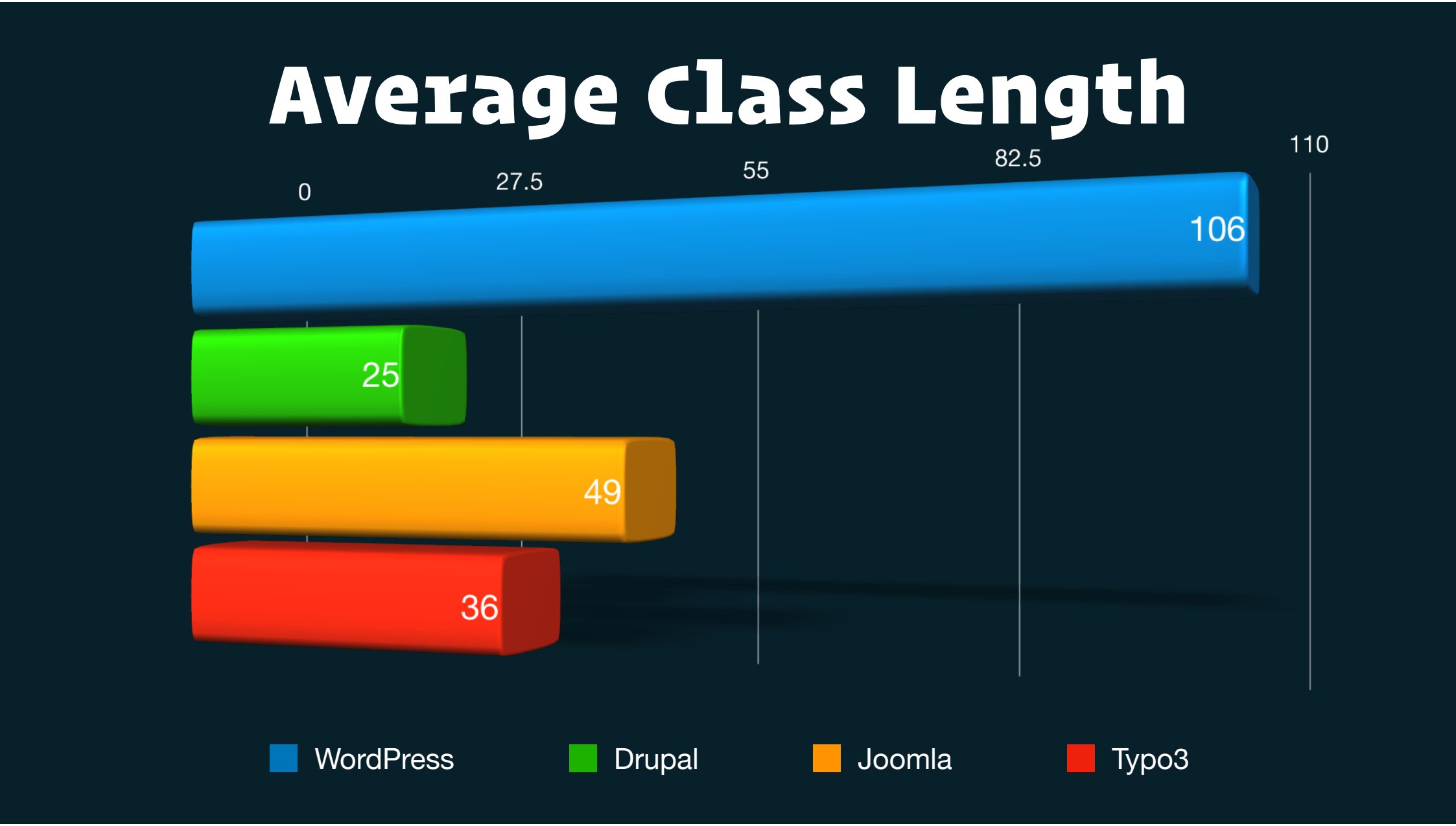
Time Magazine 📰

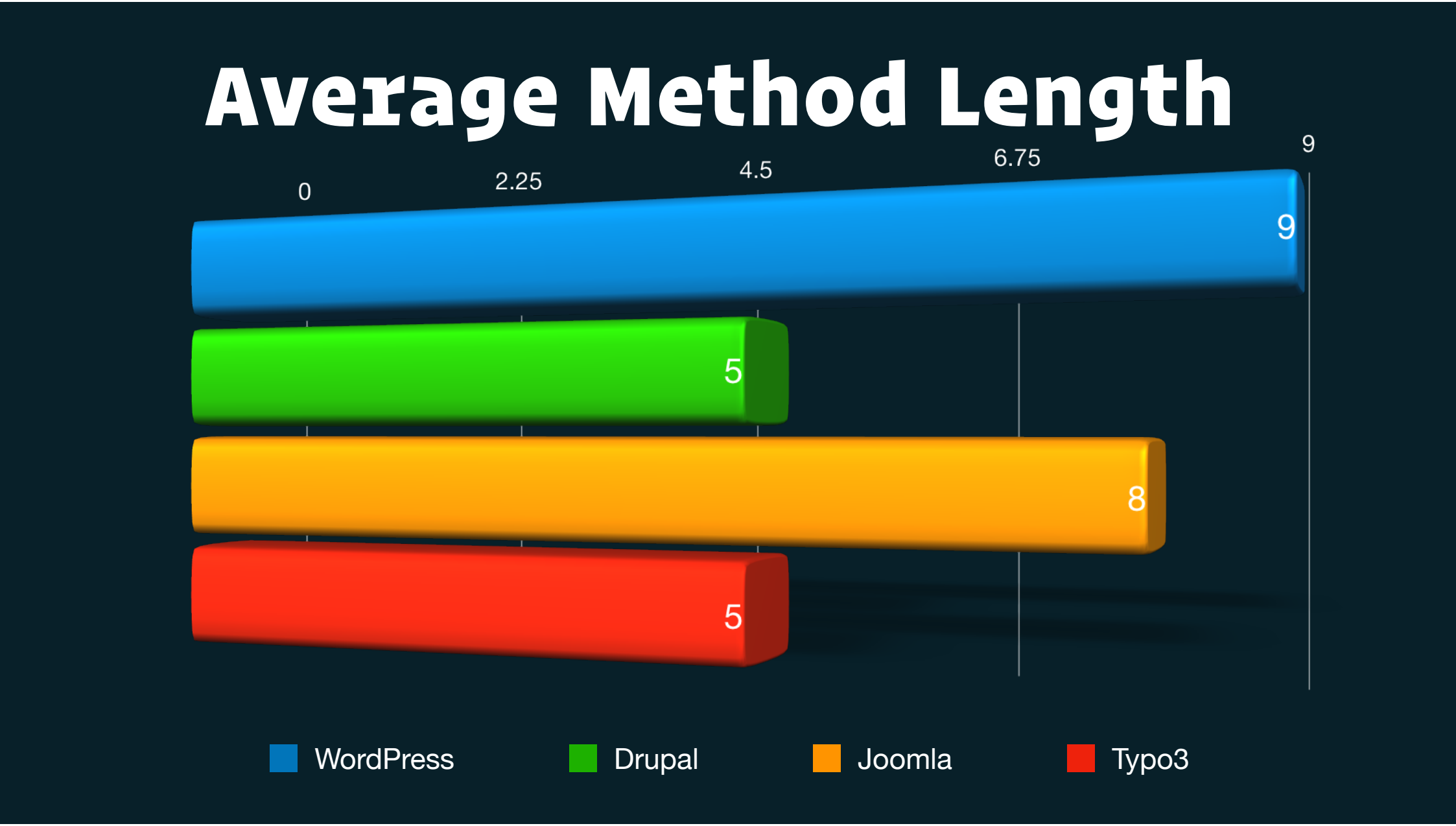
Sony Music 🎤

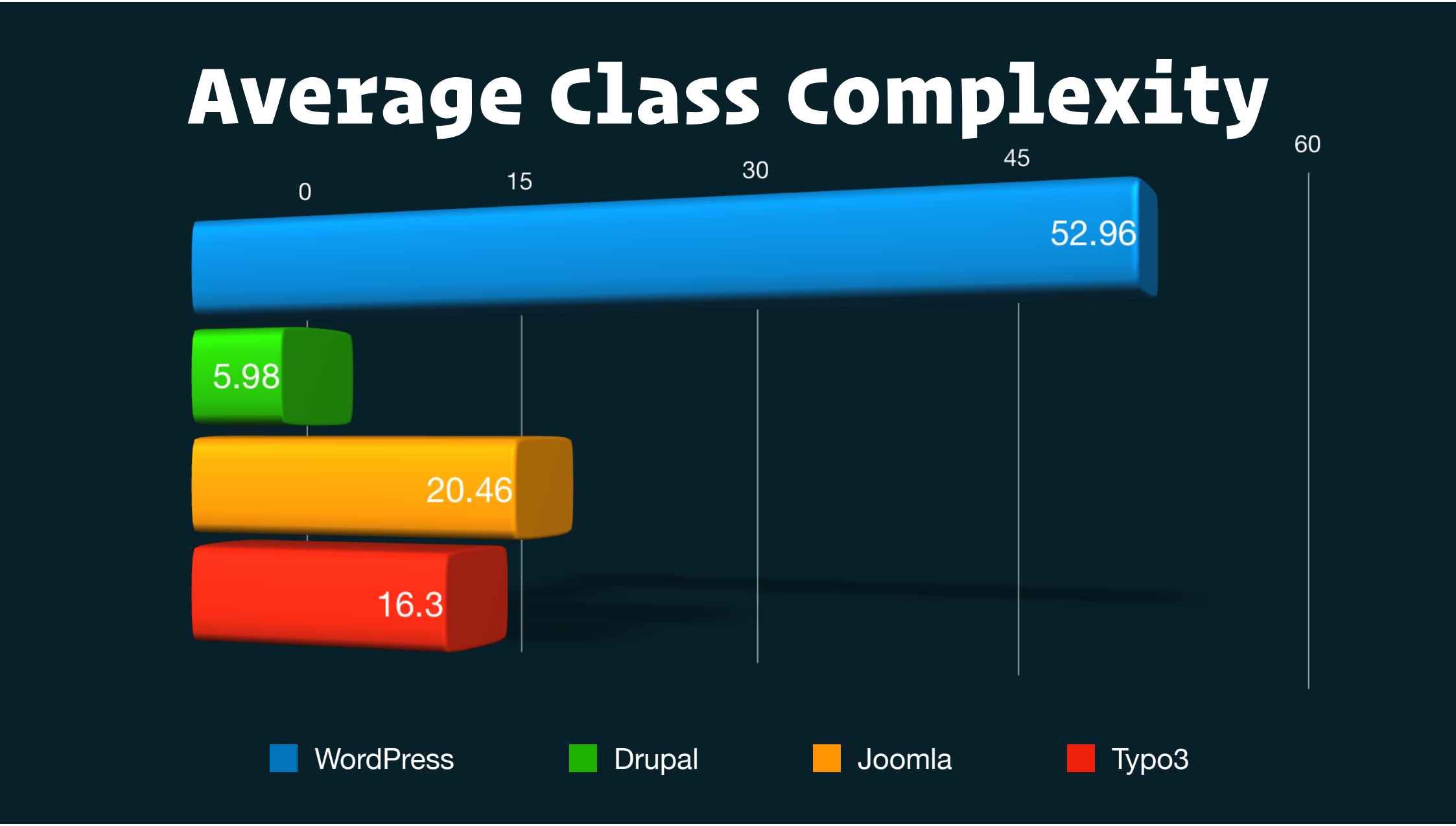
Source https://wordpress.org/showcase/


WORDPRESS
IS THA SHIZZLE
imgflip.com

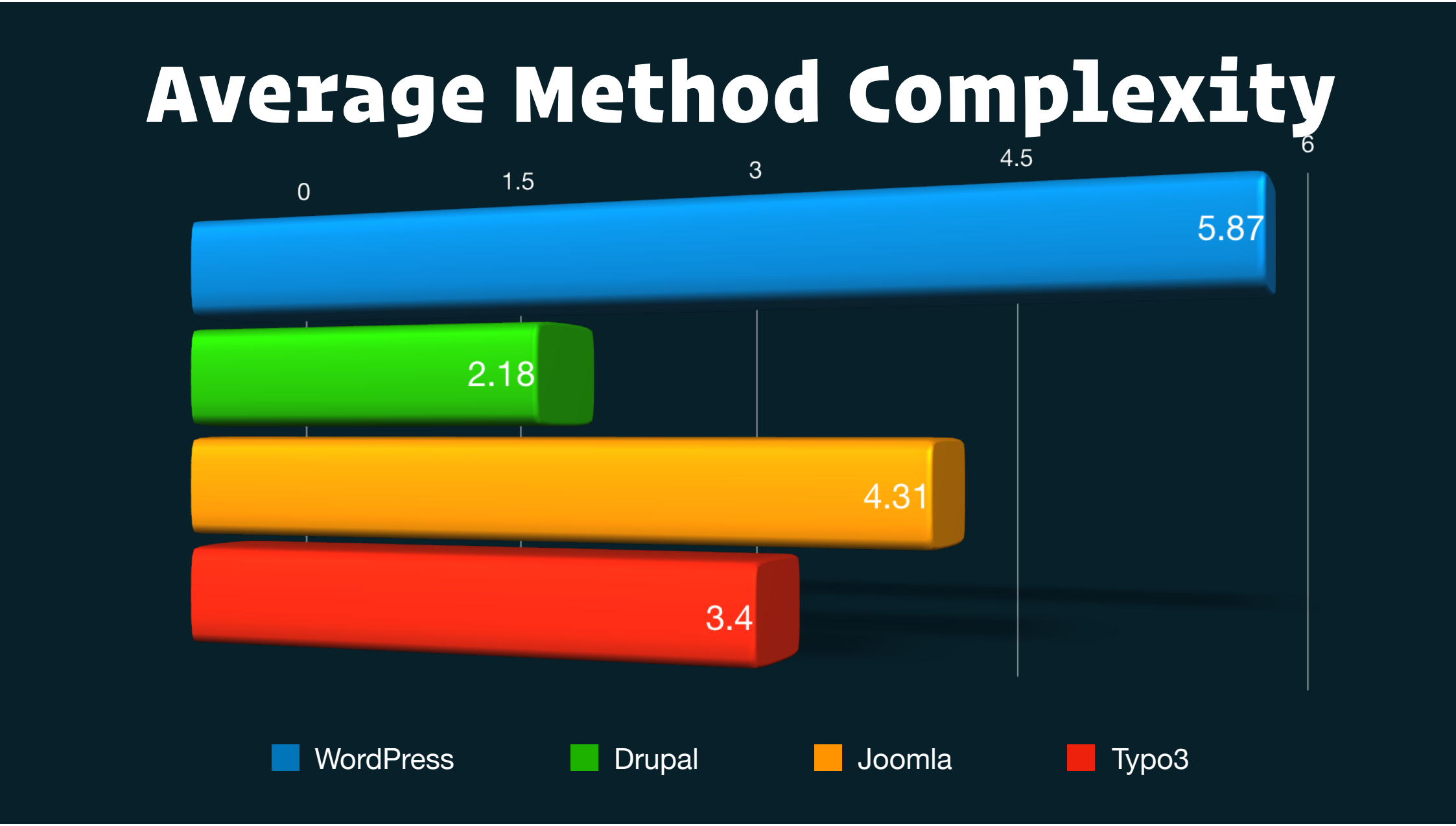

Lines of Code
0
350000
700000
1050000
1400000
343,186
1,305,555
570,901
596,175
WordPress
Drupal
Joomla
Typo3

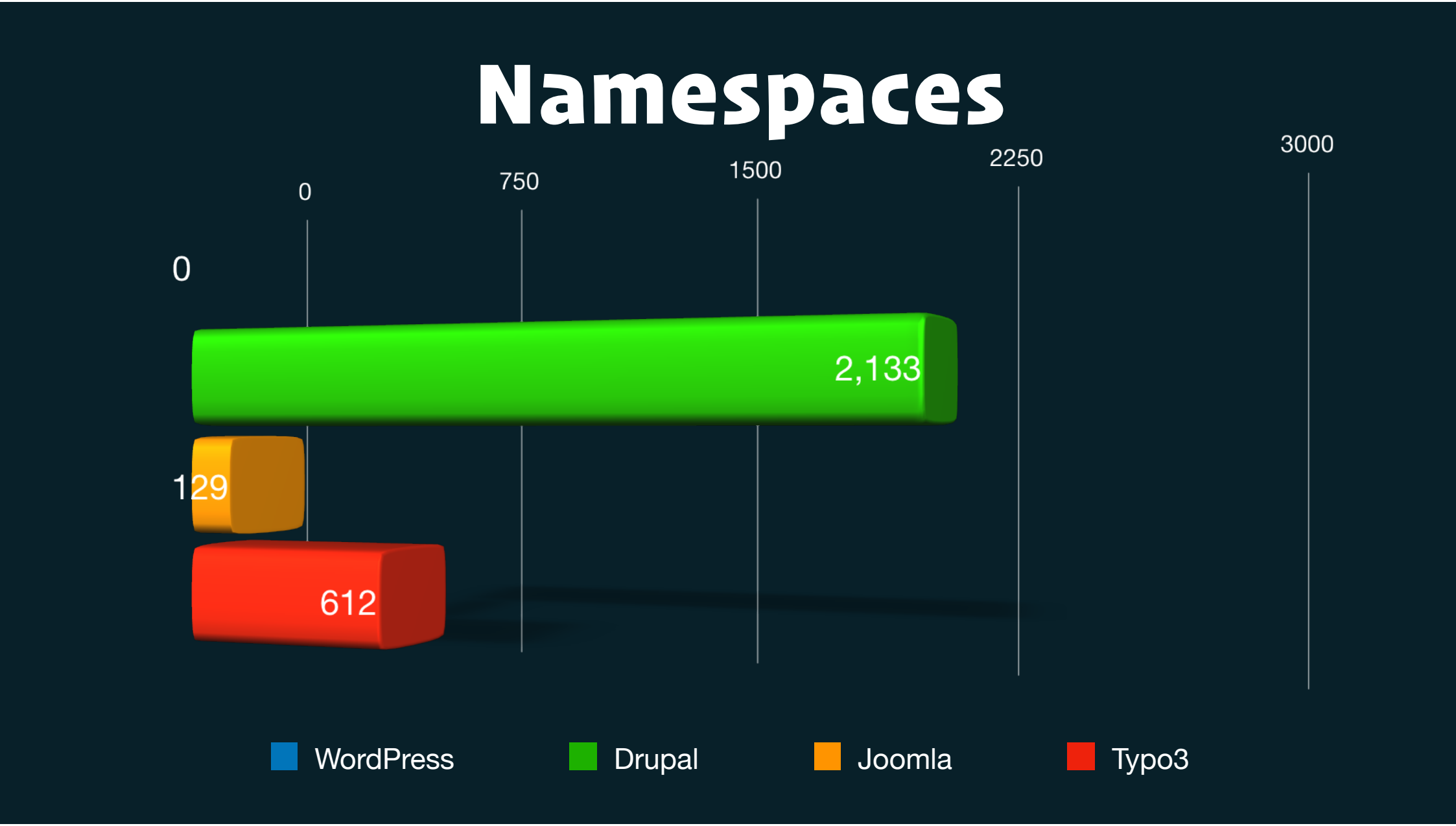

Average Class Length
0
27.5
55
82.5
110
106
25
49
36
WordPress
Drupal
Joomla
Typo3


Average Method Length
0
2.25
4.5
6.75
9
9
5
8
5
WordPress
Drupal
Joomla
Typo3


Average Class Complexity
0
15
30
45
60
52.96
5.98
20.46
16.3
WordPress
Drupal
Joomla
Typo3

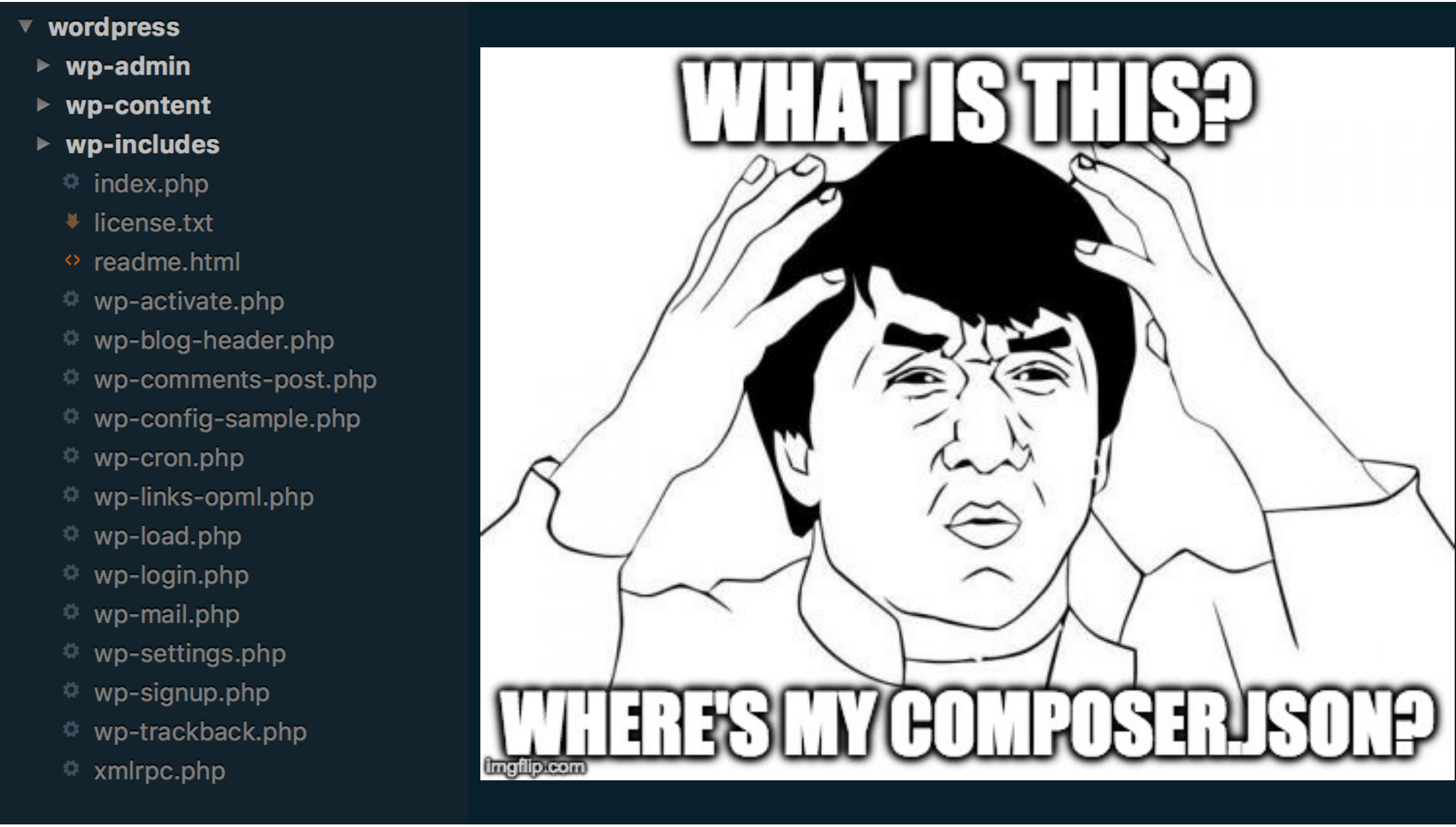
Average Method Complexity



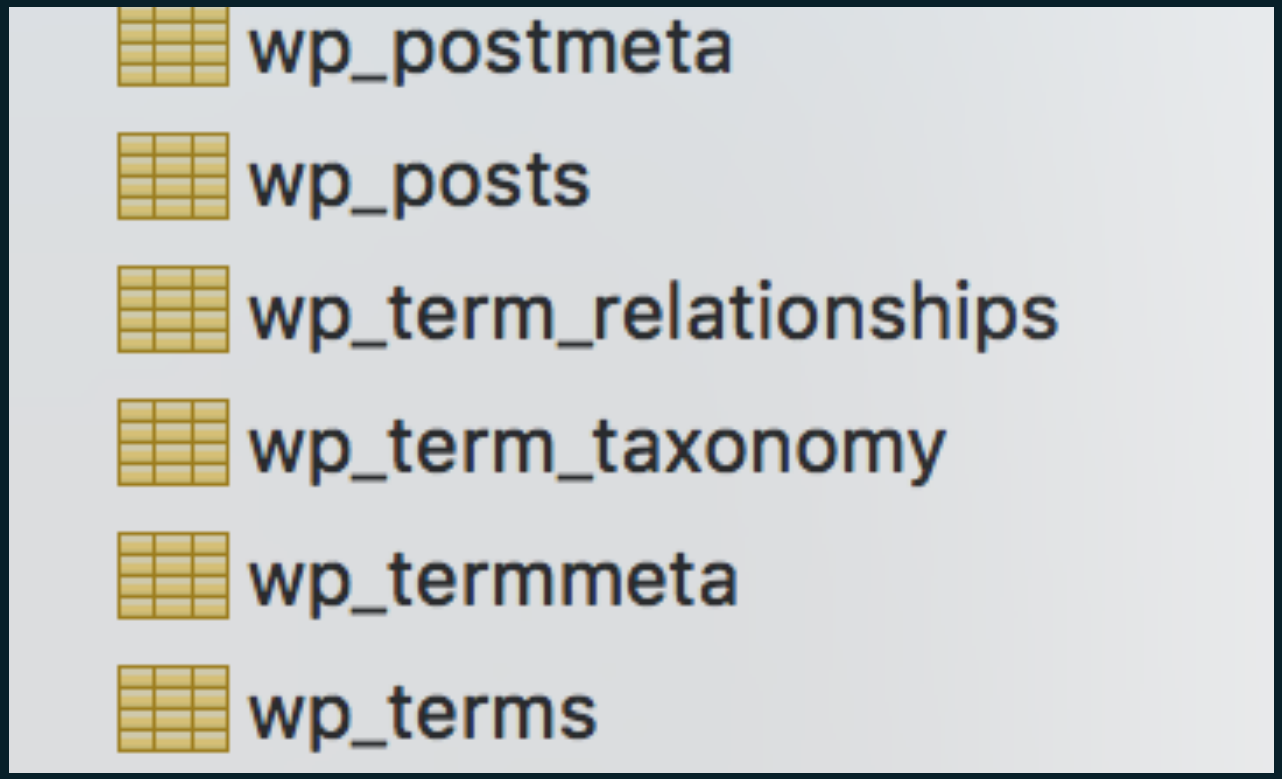

Namespaces
0
750
1500
2250
3000
0
2,133
129
612
WordPress
Drupal
Joomla
Typo3

Developer's POV 👩‍💻

It’s not a CMS.


wordpress
wp-admin
wp-content
wp-includes
index.php
license.txt
readme.html
wp-activate.php
wp-blog-header.php
wp-comments-post.php
wp-config-sample.php
wp-cron.php
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
xmlrpc.php
WHAT IS THIS?
WHERE'S MY COMPOSER.JSON?
imgflip.com


// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');
/** MySQL database username */
define('DB_USER', 'root');
/** MySQL database password */
define('DB_PASSWORD', 'root');
/** MySQL hostname */
define('DB_HOST', 'localhost');
wp-config.php
Great for pushing to a repository. Not.



ID
post_author
post_date
post_date_gmt
post_content
post_title
post_excerpt
post_status
comment_status
ping_status
post_password
post_name
to_ping
pinged

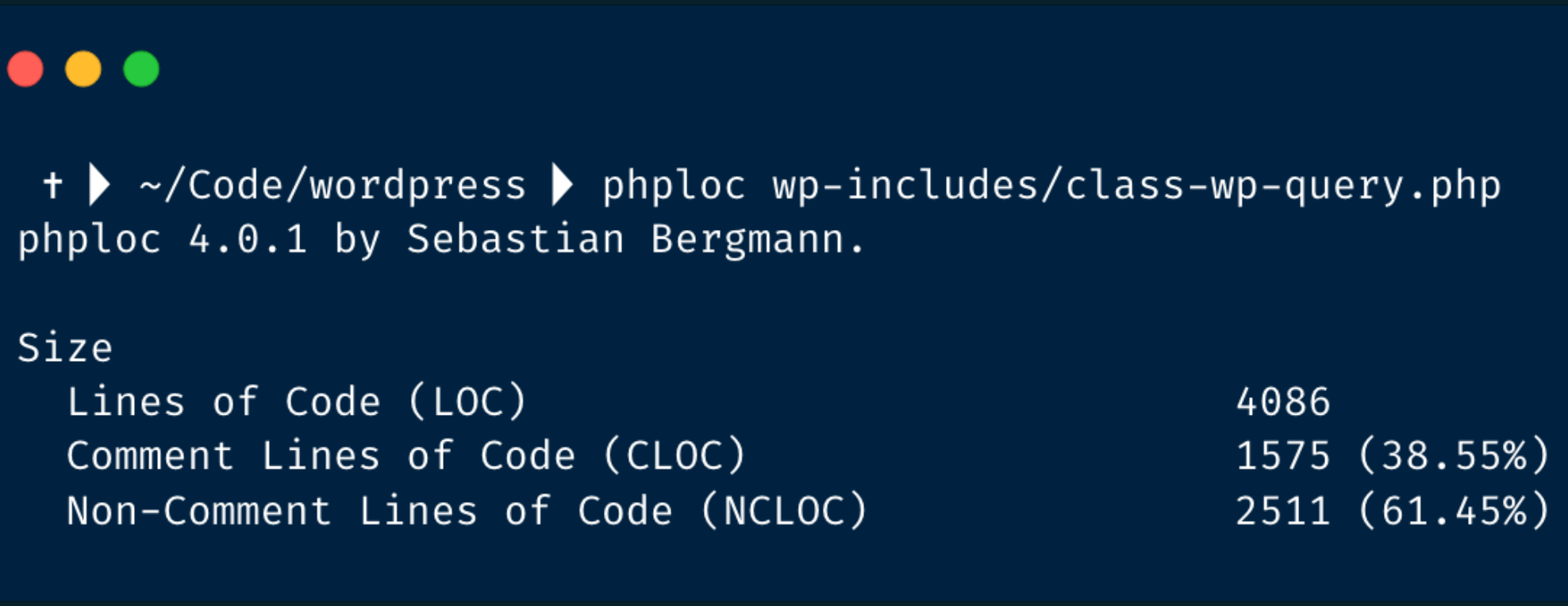
Tables and Columns

They speak for themselves. Don't they?

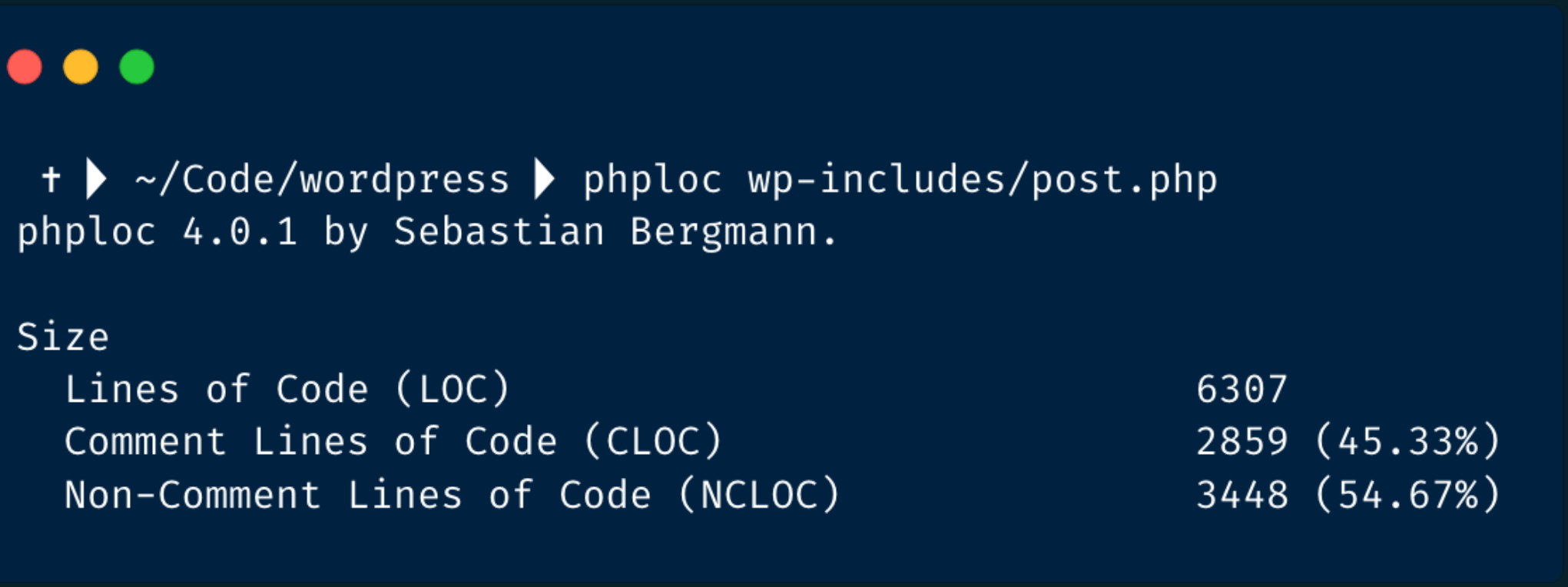
```php
// 1st Method - Declaring $wpdb as global and using it to execute an SQL query statement that returns a PHP object

global $wpdb;
$results = $wpdb->get_results( "SELECT * FROM {$wpdb->prefix}options WHERE option_id = 1", OBJECT );

// 2nd Method - Utilizing the $GLOBALS superglobal. Does not require global keyword ( but may not be best practice )

$results = $GLOBALS['wpdb']->get_results( "SELECT * FROM {$wpdb->prefix}options WHERE option_id = 1", OBJECT );
```

Globals FTW!

Source https://codex.wordpress.org/Class_Reference/wpdb



Small classes



Even smaller classes

```
// Do not delete these lines
    if (!empty($_SERVER['SCRIPT_FILENAME']) && 'comments.php' == basename($_SERVER['SCRIPT_FILENAME']))
        die ('Please do not load this page directly. Thanks!');
```

Helpful comments are helpful

```
<section class="no-results not-found">
    <header class="page-header">
        <h1 class="page-title"><?php _e( 'Nothing Found', 'twentyfifteen' ); ?></h1>
    </header><!-- .page-header -->

    <div class="page-content">

        <?php if ( is_home() && current_user_can( 'publish_posts' ) ) : ?>

            <p><?php printf( __( 'Ready to publish your first post? <a href="%1$s">Get started here</a>.', 'twentyfifteen' ), esc_url( admin_url( 'post-new.php' ) ) );
?></p>

        <?php elseif ( is_search() ) : ?>

            <p><?php _e( 'Sorry, but nothing matched your search terms. Please try again with some different keywords.', 'twentyfifteen' ); ?></p>
            <?php get_search_form(); ?>

        <?php else : ?>

            <p><?php _e( 'It seems we can&rsquo;t find what you&rsquo;re looking for. Perhaps searching can help.', 'twentyfifteen' ); ?></p>
            <?php get_search_form(); ?>

        <?php endif; ?>

    </div><!-- .page-content -->
</section><!-- .no-results -->
```

Themes

Magic Numbers 

```php
switch ( $action ) {
    case "upgrade":
        $n = ( isset($_GET['n']) ) ? intval($_GET['n']) : 0;

        if ( $n < 5 ) {
```

```php
for ( $i = 0; $i < 50 && $parent > 0; $i++ ) {
            $children[] = $parent;

            foreach ( $pages as $page ) {
```

Why not 3.1415?

Vulnerabilities 🔓

WordPress FAQ

https://codex.wordpress.org/FAQ_My_site_was_hacked

78% of hacked websites in Q1 2016 used WordPress

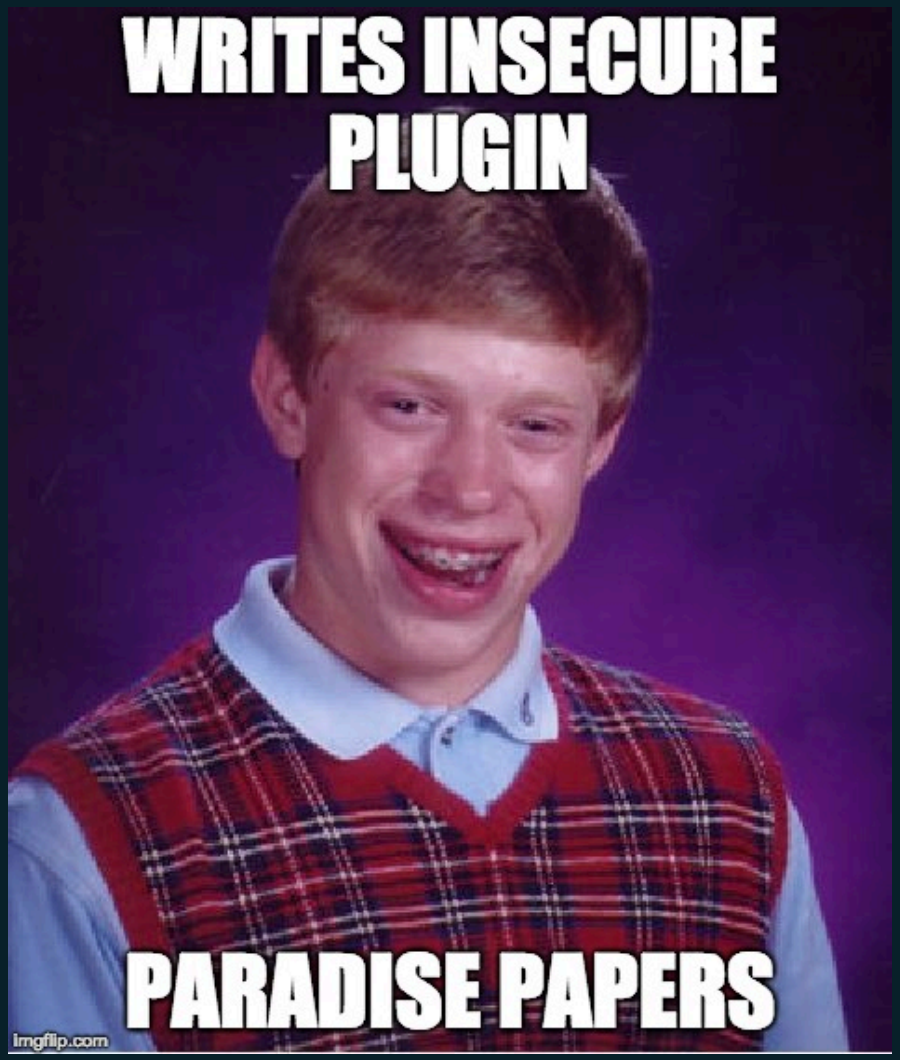
Source https://sucuri.net/infographics/

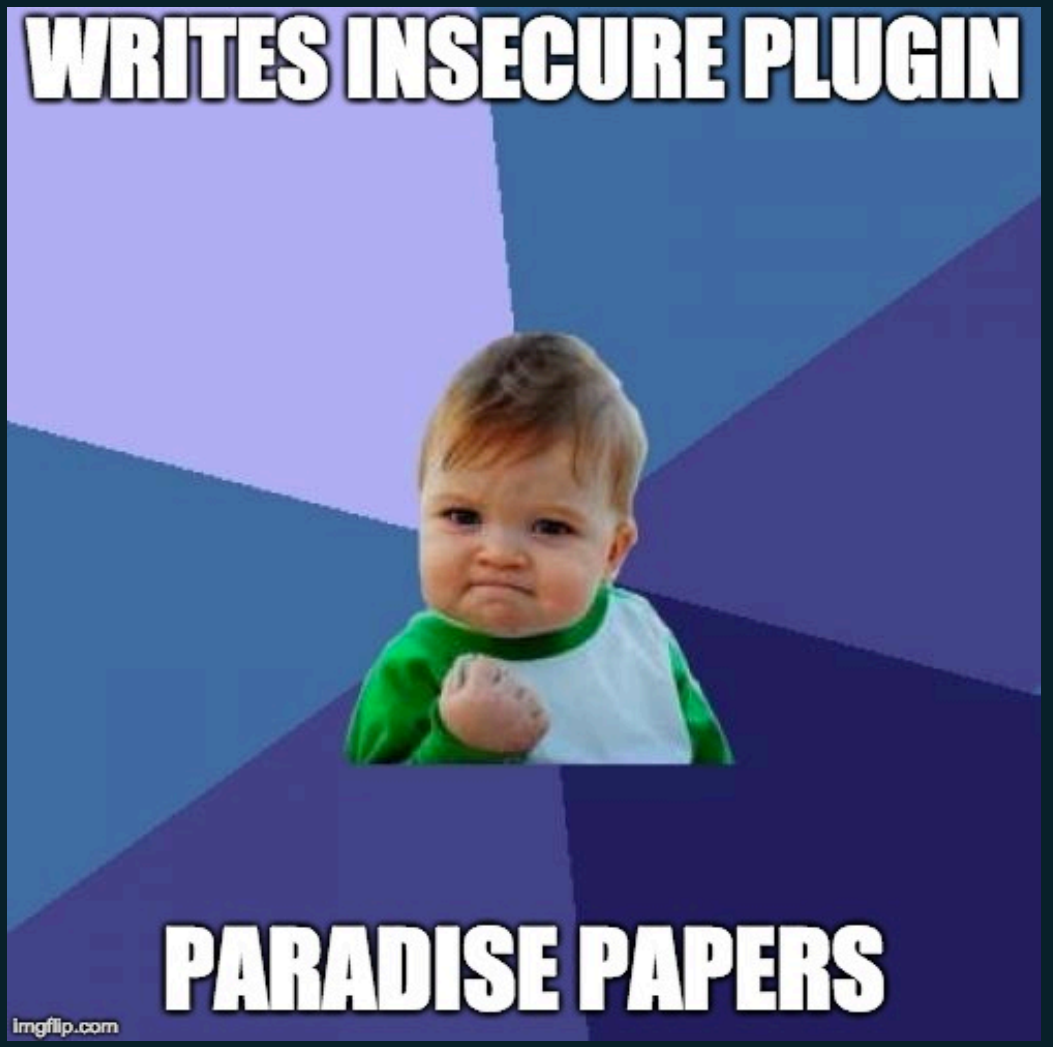
Mossack Fonseca Breach – WordPress Revolution Slider Plugin Possible Cause

This entry was posted in General Security, WordPress Security on April 7, 2016 by Mark Maunder 54 Replies

Update: We have written a follow-up post on how an attacker may have moved laterally on the network from WordPress into the email server.

Source: https://www.wordfence.com/blog/2016/04/mossack-fonseca-breach-vulnerable-slider-revolution/


WRITES INSECURE PLUGIN
PARADISE PAPERS
imgflip.com


WRITES INSECURE PLUGIN
PARADISE PAPERS
imgflip.com

Security Through Obscurity

Hide the “admin” user.

Change the default table prefix.

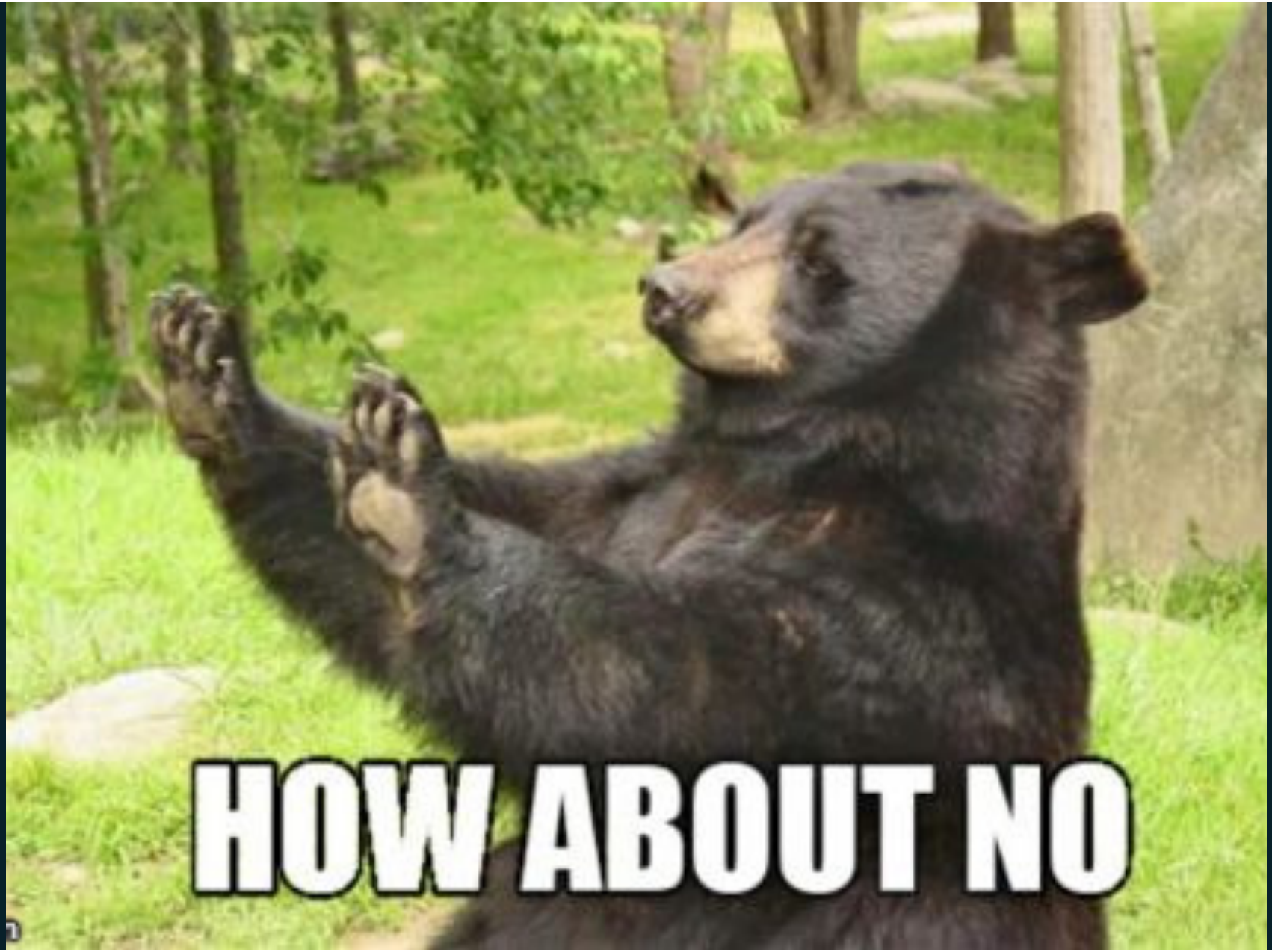
Hide the login page.

Hide the WordPress version.

Rename the wp_ folders.

Hide WordPress altogether.

Source https://blogvault.net/wordpress-security-through-obscurity/


HOW ABOUT NO

Passwords

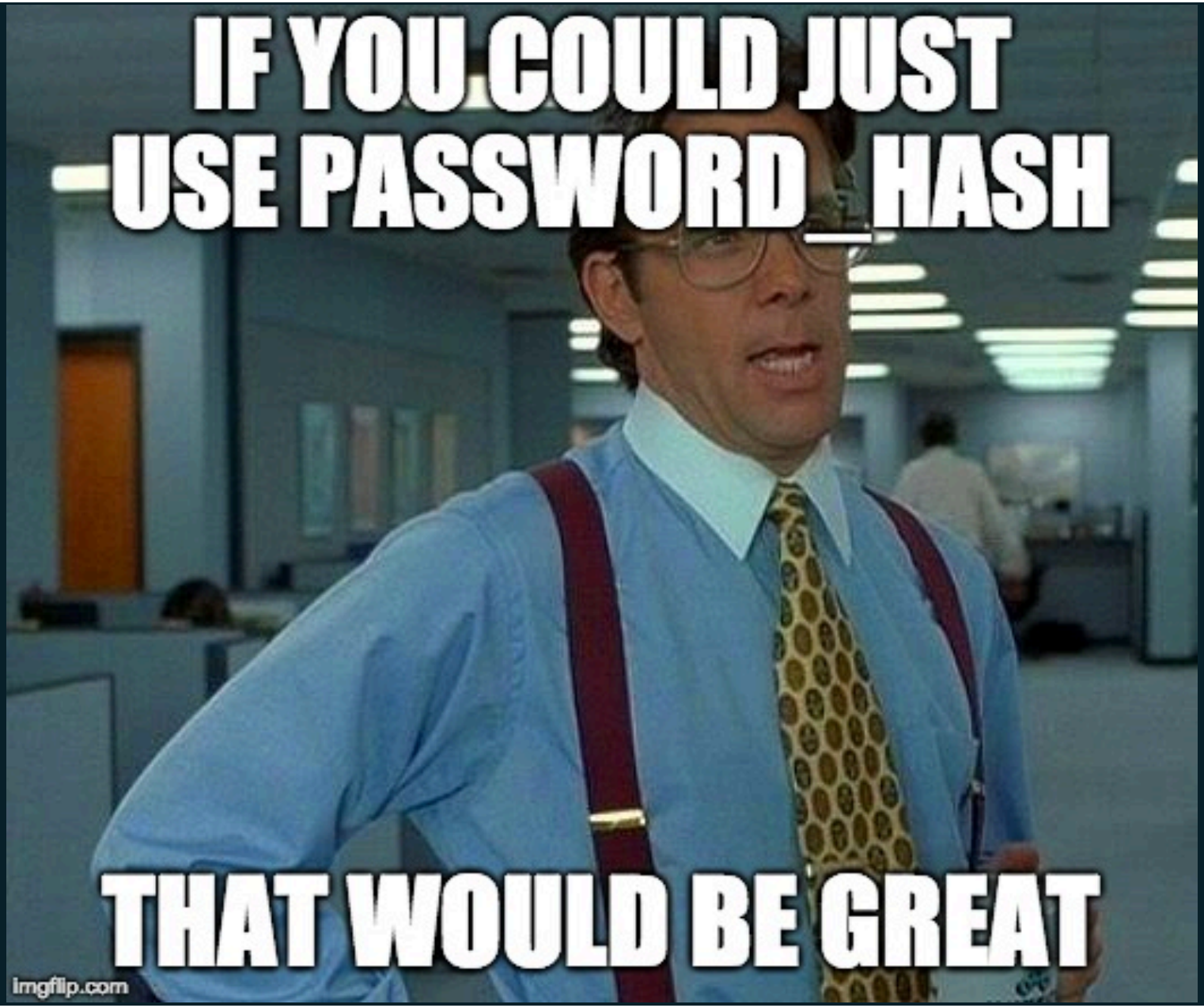
WordPress relies on the Portable PHP password hashing framework

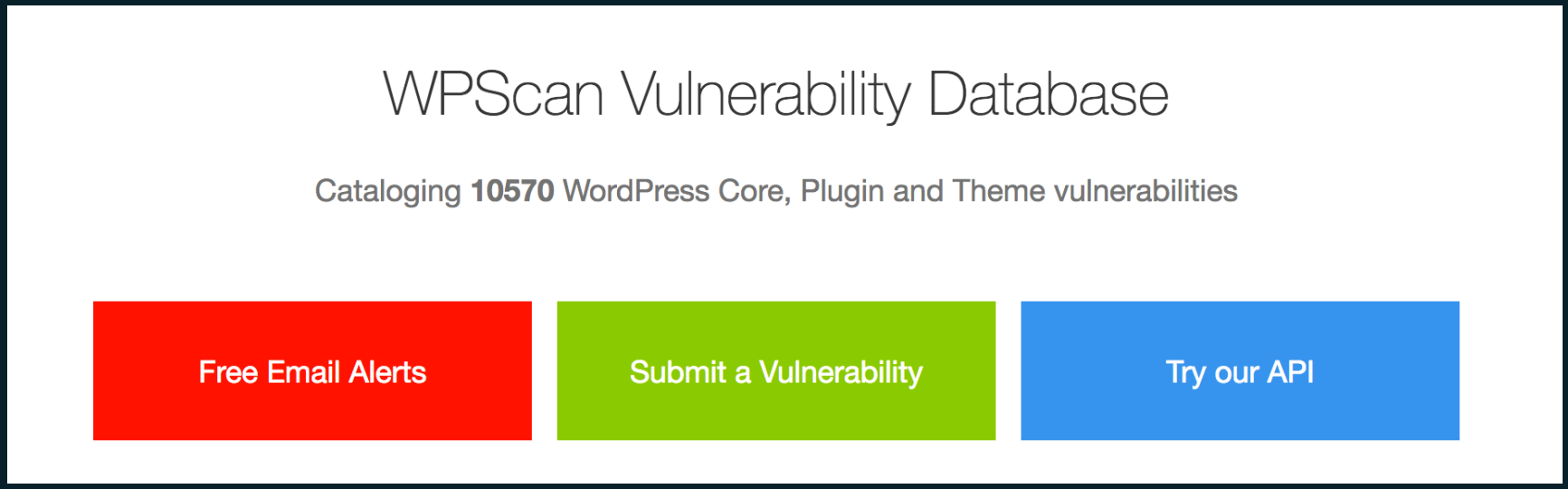
MD5 as a fallback

Password hashes don’t get “upgraded” after login

Passwords

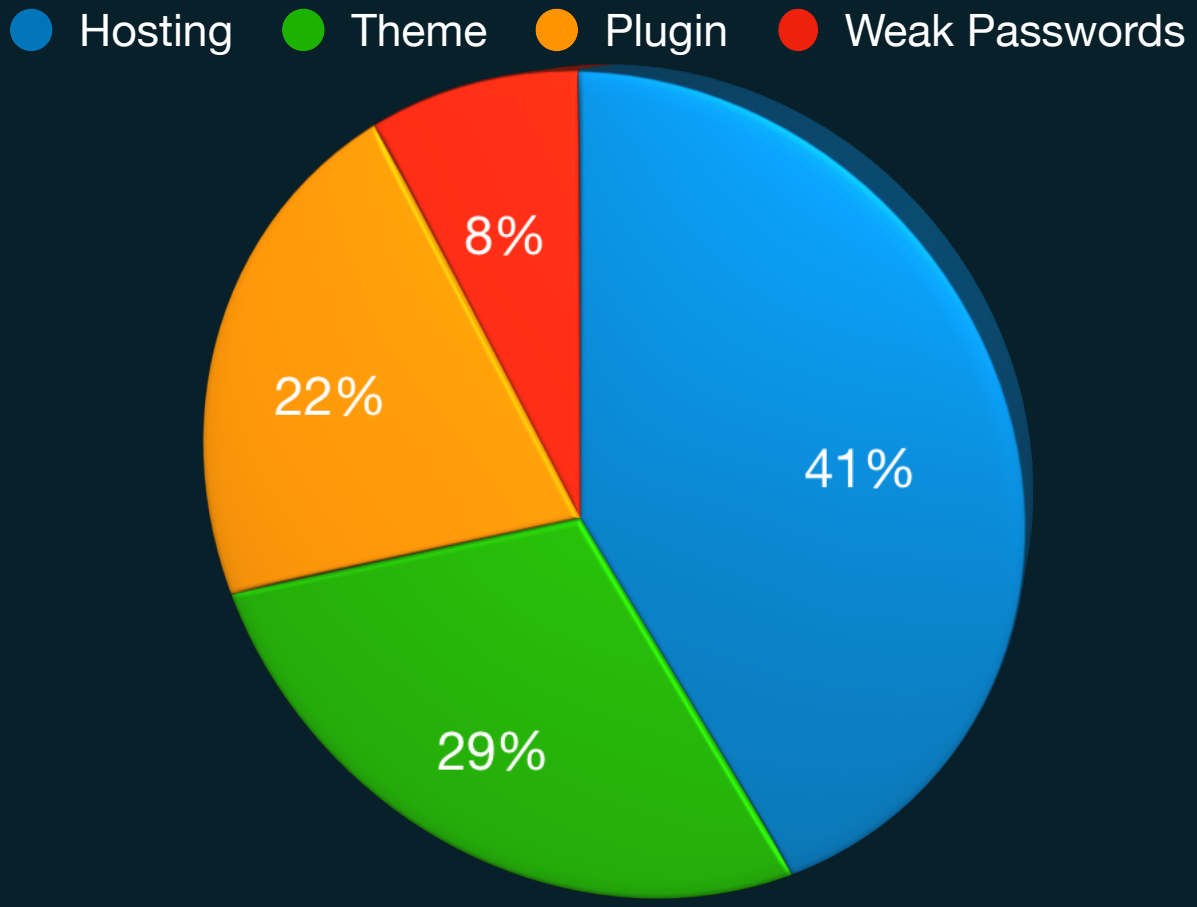
```
# We're kind of forced to use MD5 here since it's the only
# cryptographic primitive available in all versions of PHP
# currently in use.  To implement our own low-level crypto
# in PHP would result in much worse performance and
# consequently in lower iteration counts and hashes that are
# quicker to crack (by non-PHP code).
```


IF YOU COULD JUST
USE PASSWORD_HASH
THAT WOULD BE GREAT
imgflip.com



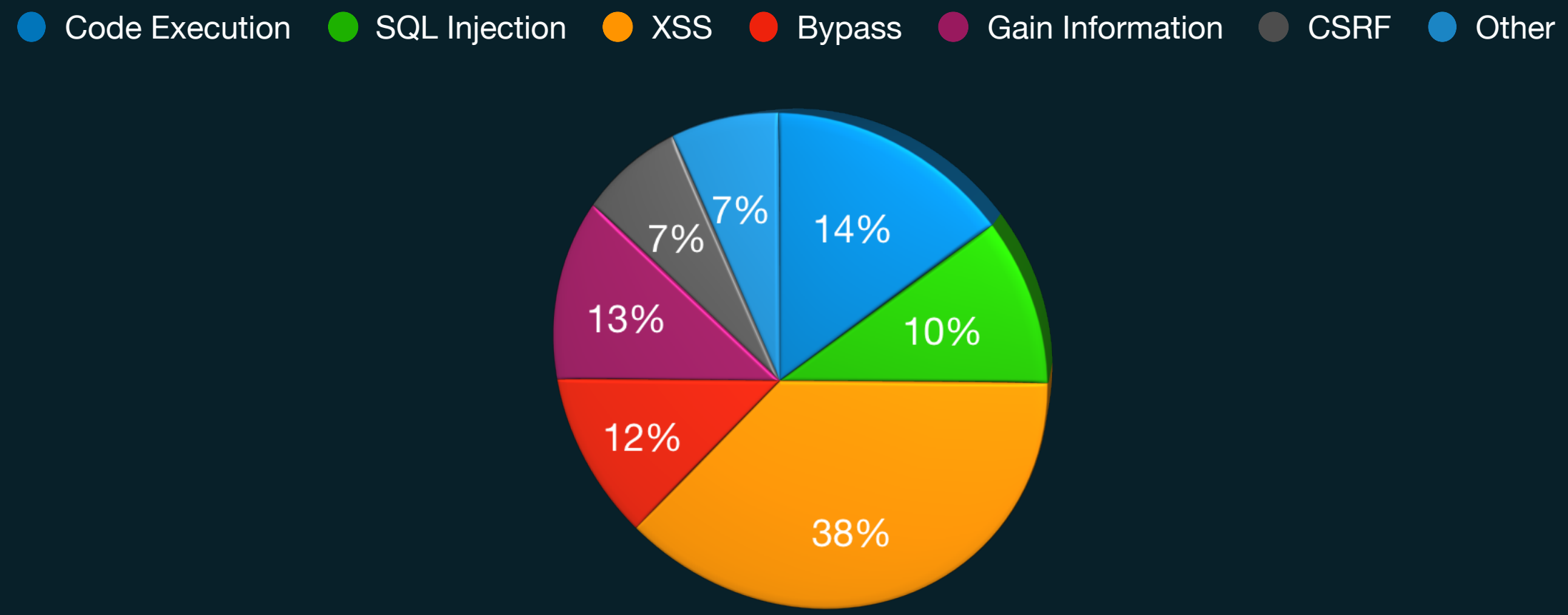
https://wpvulndb.com

Attack Vectors



Source https://torquemag.io/2016/03/wordpress-sites-hacked/

CVE (Common Vulnerabilities and Exploits)



Source http://www.cvedetails.com/product/4096/Wordpress-Wordpress.html?vendor_id=2337

Conclusion 🏁

Database column’s names are a mess (e.g. post_author is an ID).

Spaghetti code EVERYWHERE. Magic Numbers all the time.

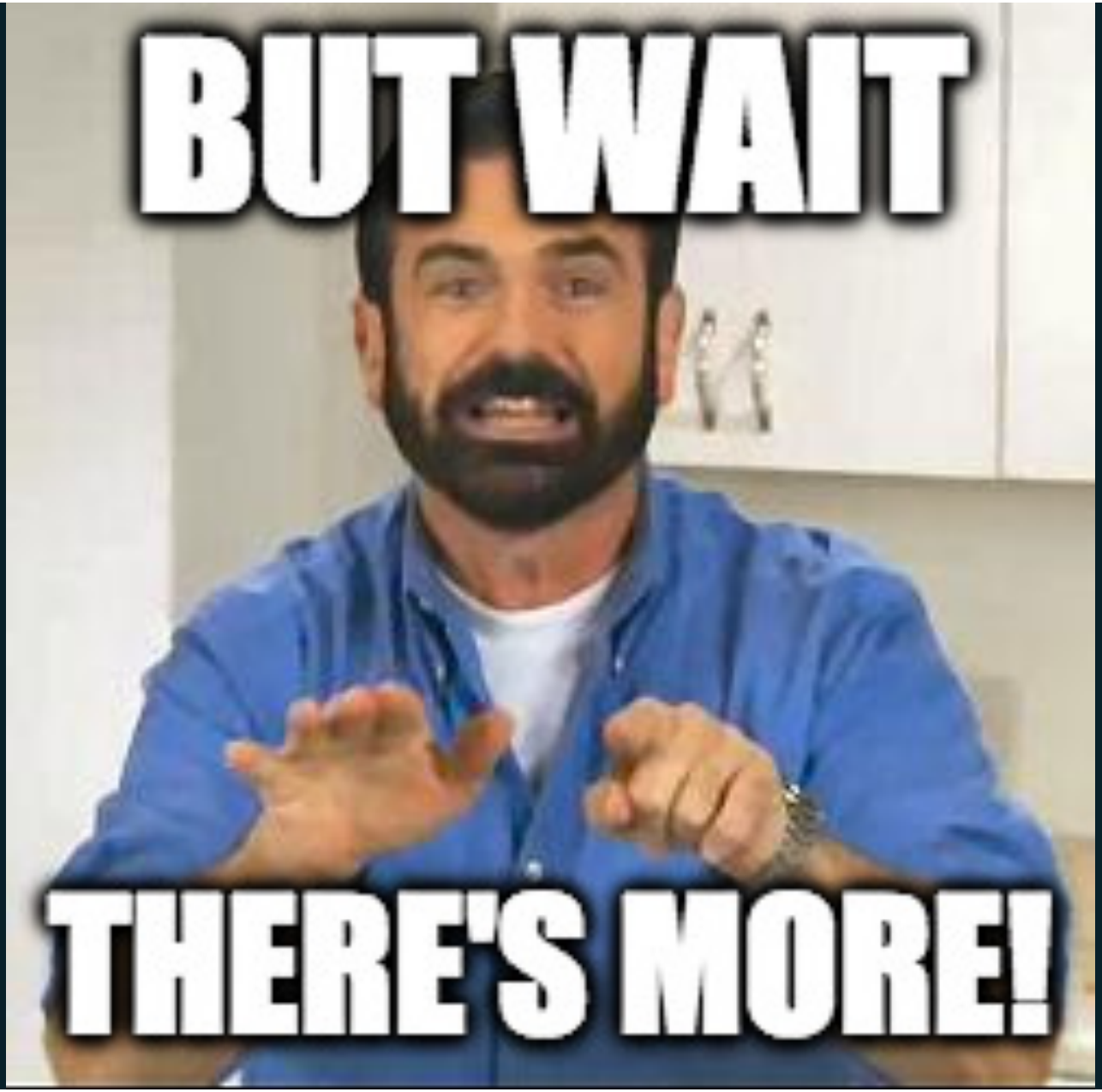
No separation of concerns (MVC).

Super-long classes (4.000 LOC and up).

Different coding styles throughout the codebase. Sometimes within the same class.

Querying the database hurts your brain.

Only MySQL/MariaDB-Support out of the box.


BUT WAIT
THERE'S MORE!

No templating engine.

Writing plugins is cumbersome.

Writing custom templates too.

The built-in WYSIWYG editor is a mess.

Inconsistent function names.

SEO is often painful.

Absolute paths in database (mysite.com/about).

Recommendations

Use WordPress if you **must**

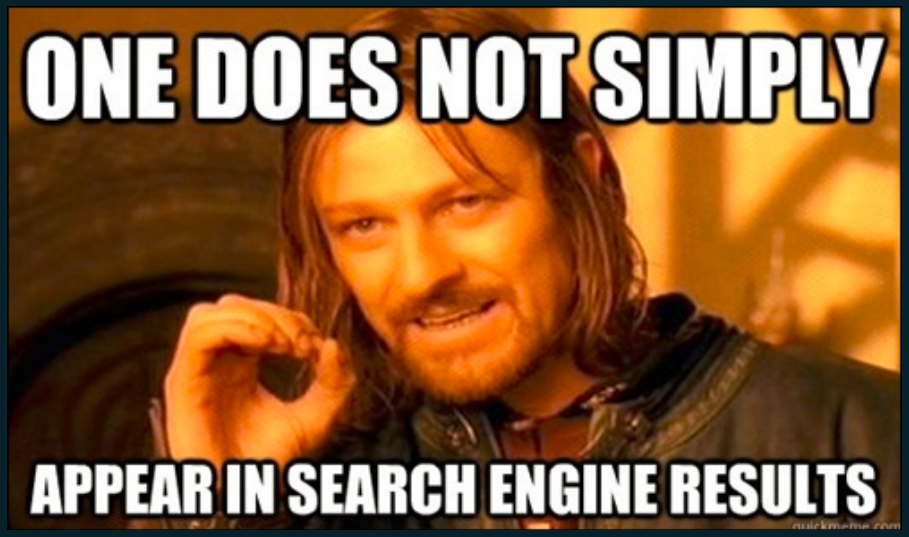
Be proactive and update often. Really often

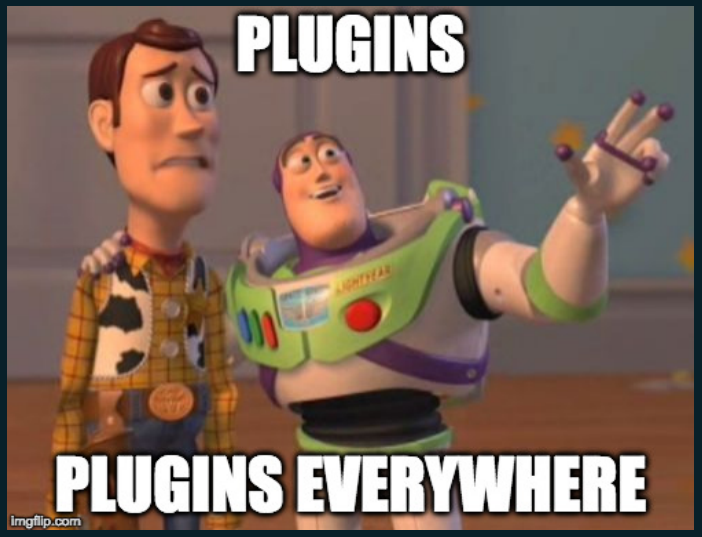
Secure your setup

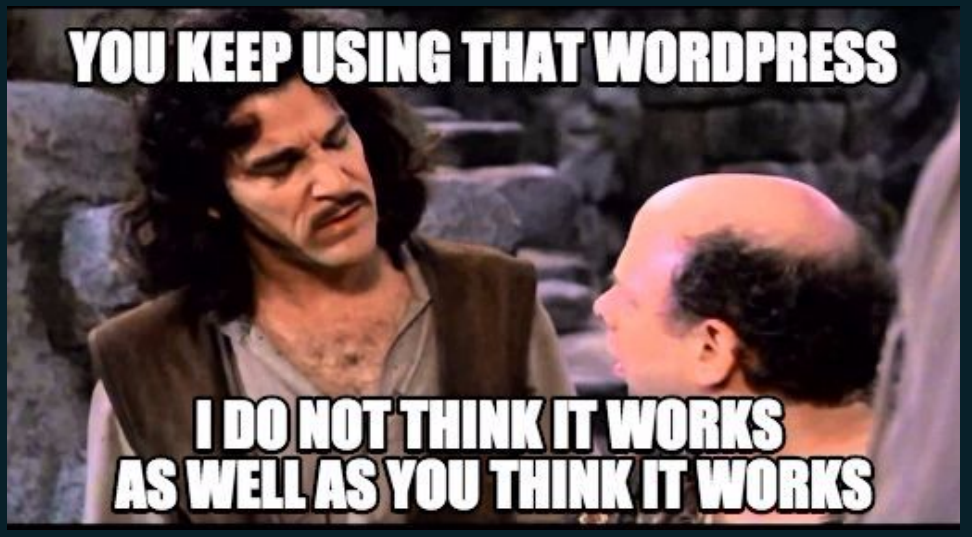
Be careful when using 3rd party plugins for they may be vulnerable

Use a real CMS (Typo3, Drupal, Joomla, OctoberCMS, Statamic etc.) if you **can**


OH, SO YOU'RE A "WORDPRESS DEVELOPER"?
TELL ME MORE ABOUT THE THIRTY PLUGINS YOU USE.
memegenerator.net


ONE DOES NOT SIMPLY
APPEAR IN SEARCH ENGINE RESULTS


PLUGINS
PLUGINS EVERYWHERE
imgflip.com


YOU KEEP USING THAT WORDPRESS
I DO NOT THINK IT WORKS AS WELL AS YOU THINK IT WORKS

Done! Thanks! Questions?

Slides are available at https://speakerdeck.com/mazedlx/