Kamusta?

(*how are you*)

I’m **Dreb**

10
up

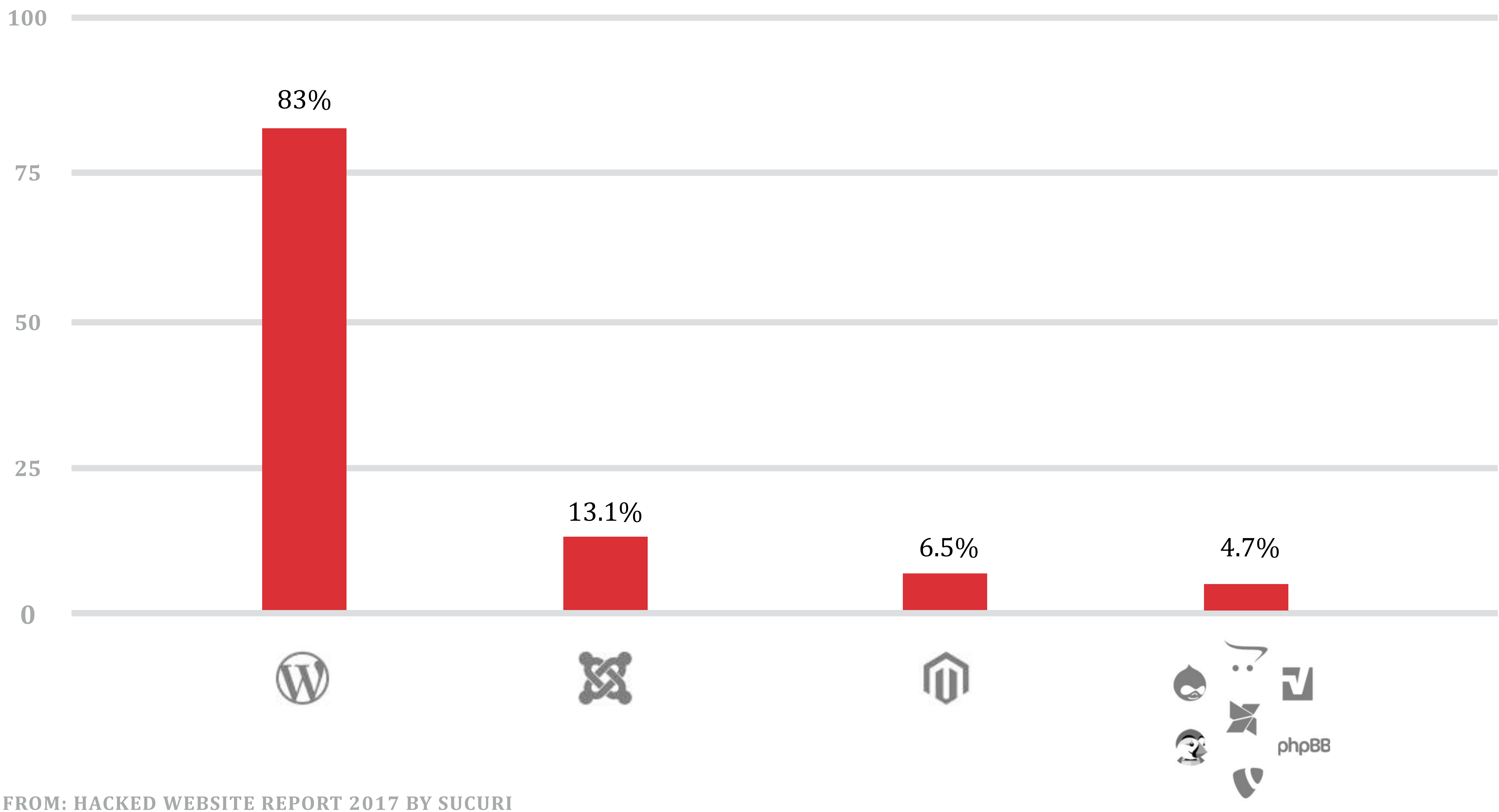
DAVAO
WordPress
DAVAO USER GROUP

WordPress
User Group Philippines

Building a better web

with Engineering Best Practices

Infected Websites Platform Distribution - 2017

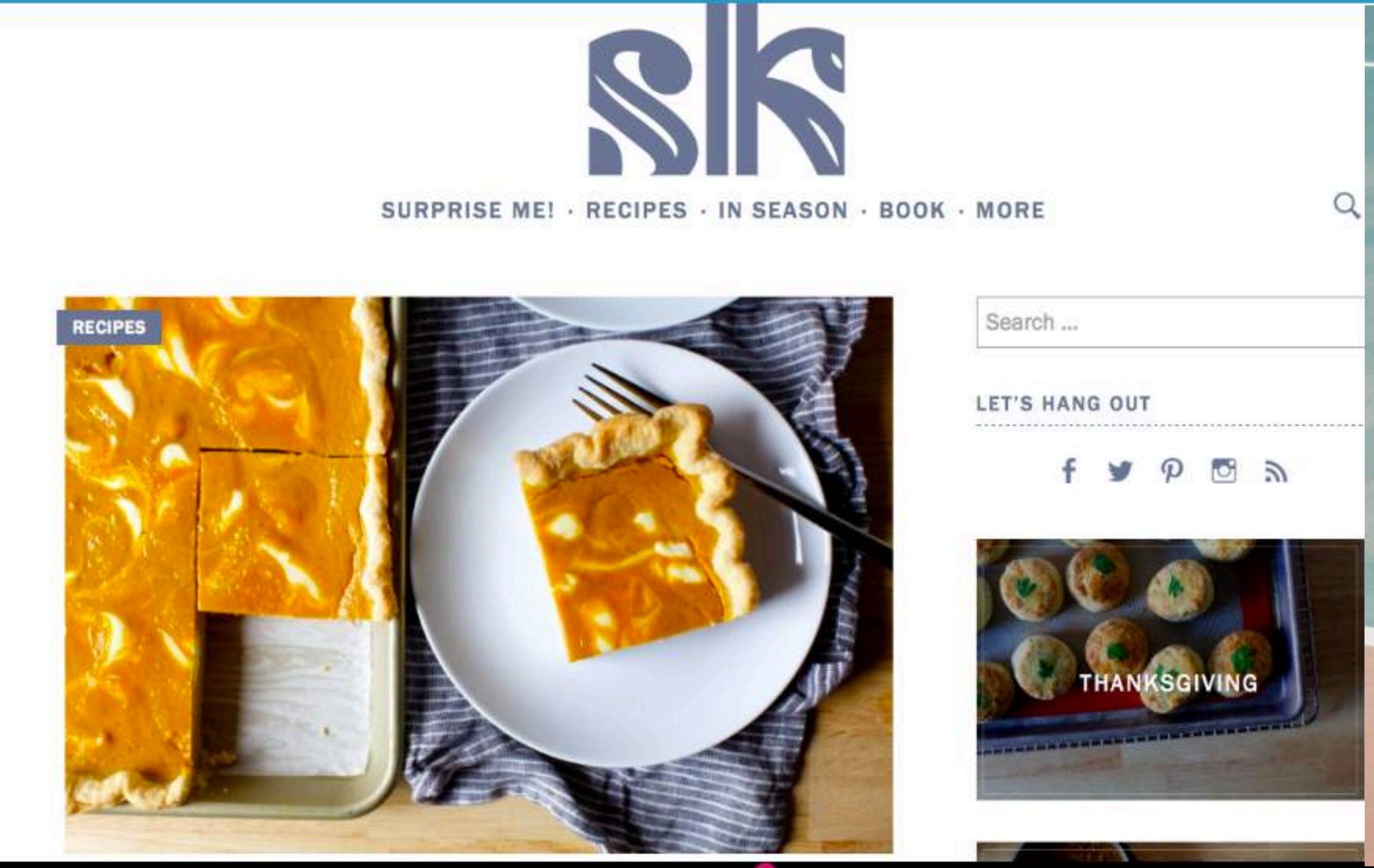


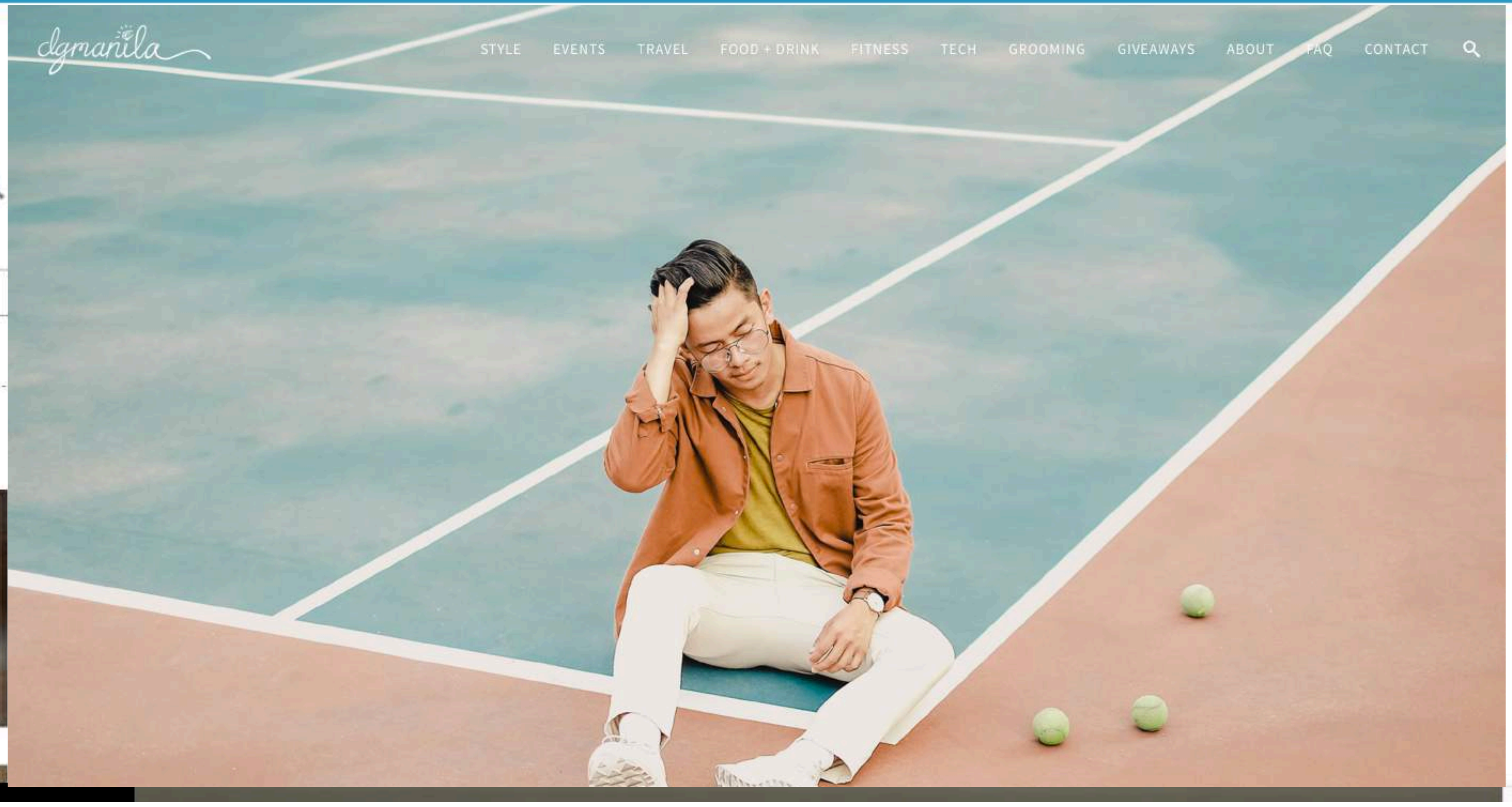
FROM: HACKED WEBSITE REPORT 2017 BY SUCURI

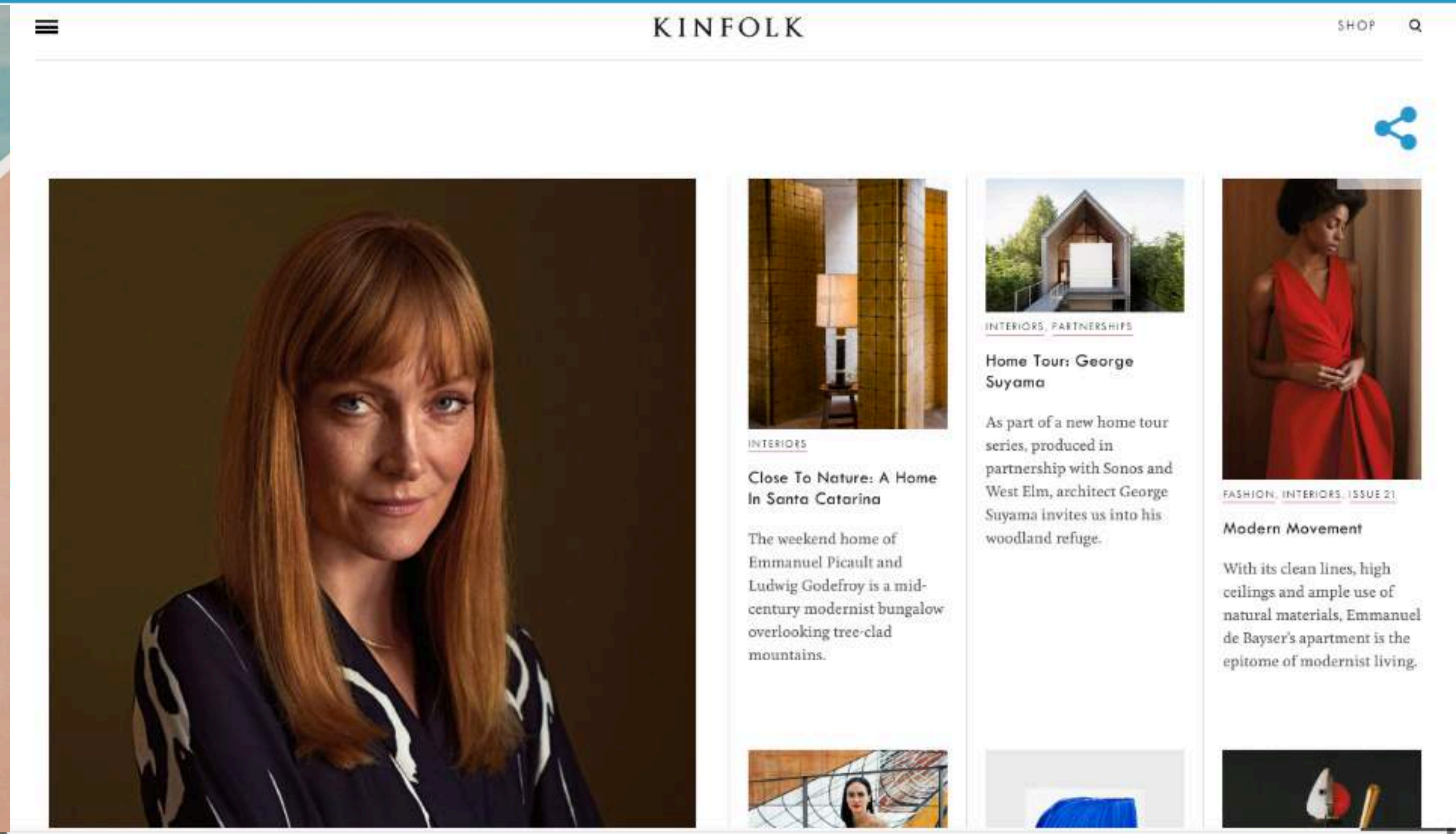
> *the compromises which were analyzed*
> *had little [if anything] to do with the core*
> *of the CMS application itself*
> *but more with its* ***improper*** *deployment,*
> *configuration and overall maintenance by the*
> *webmasters.*

FROM: HACKED WEBSITE REPORT 2017 BY SUCURI

WordPress is your blank canvas.







Close To Nature: A Home In Santa Catarina

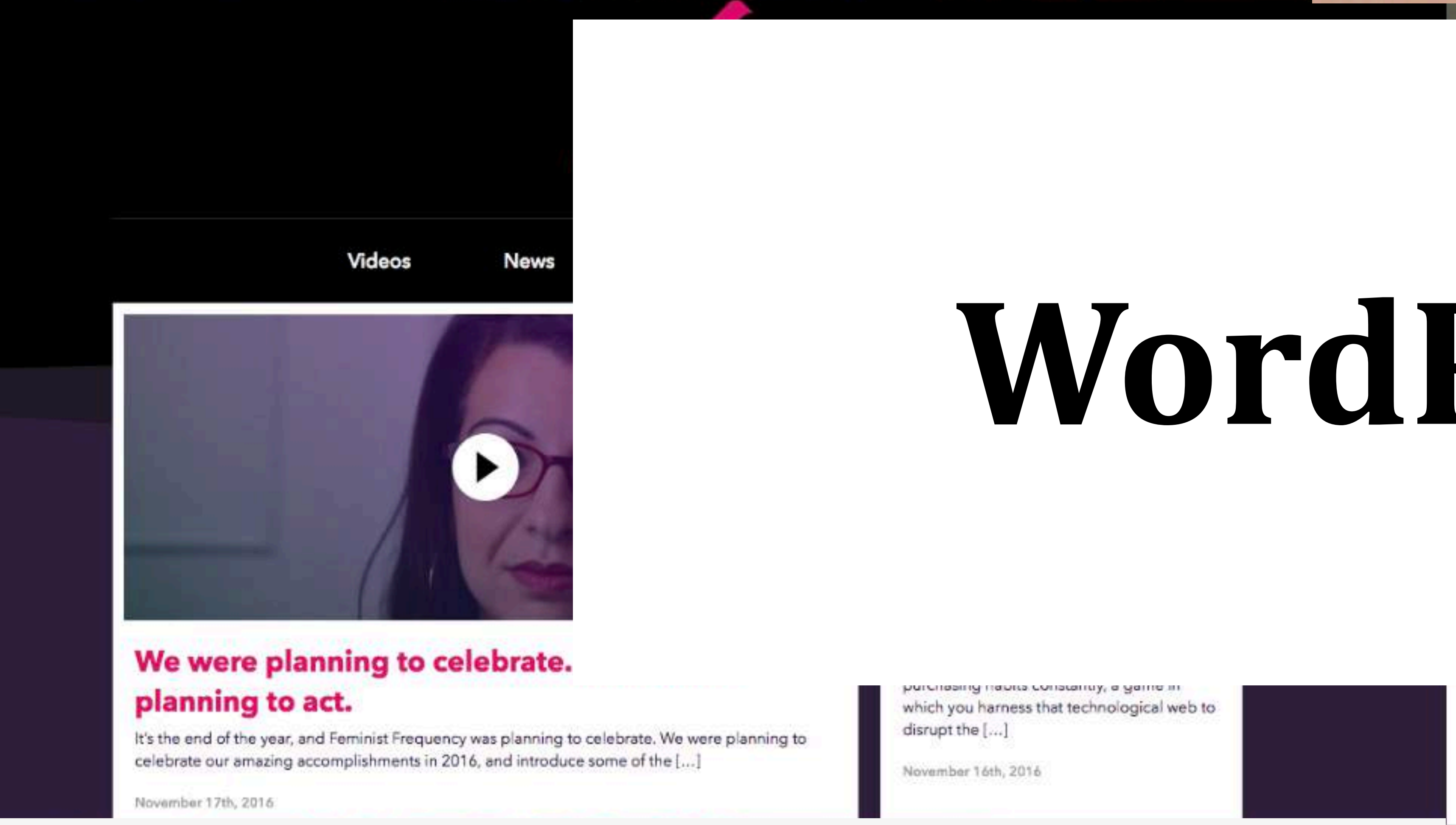
The weekend home of Emmanuel Picault and Ludwig Godefroy is a mid-century modernist bungalow overlooking tree-clad mountains.

Home Tour: George Suyama

As part of a new home tour series, produced in partnership with Sonos and West Elm, architect George Suyama invites us into his woodland refuge.

Modern Movement

With its clean lines, high ceilings and ample use of natural materials, Emmanuel de Bayser's apartment is the epitome of modernist living.



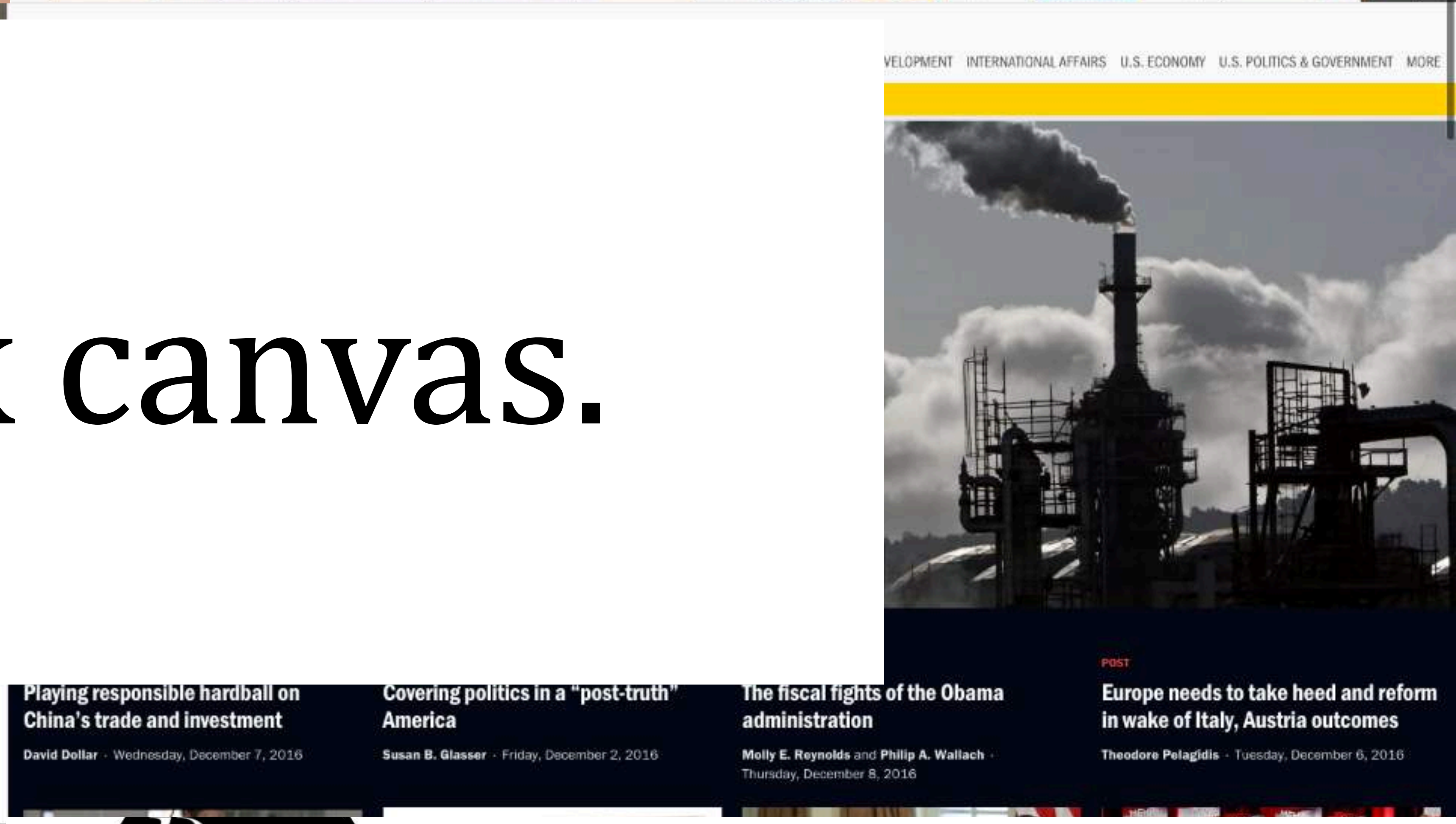
We were planning to celebrate. planning to act.

It's the end of the year, and Feminist Frequency was planning to celebrate. We were planning to celebrate our amazing accomplishments in 2016, and introduce some of the [...]

November 17th, 2016

purchasing habits constantly, a game in which you harness that technological web to disrupt the [...]

November 16th, 2016



Playing responsible hardball on China's trade and investment

David Dollar · Wednesday, December 7, 2016

Covering politics in a "post-truth" America

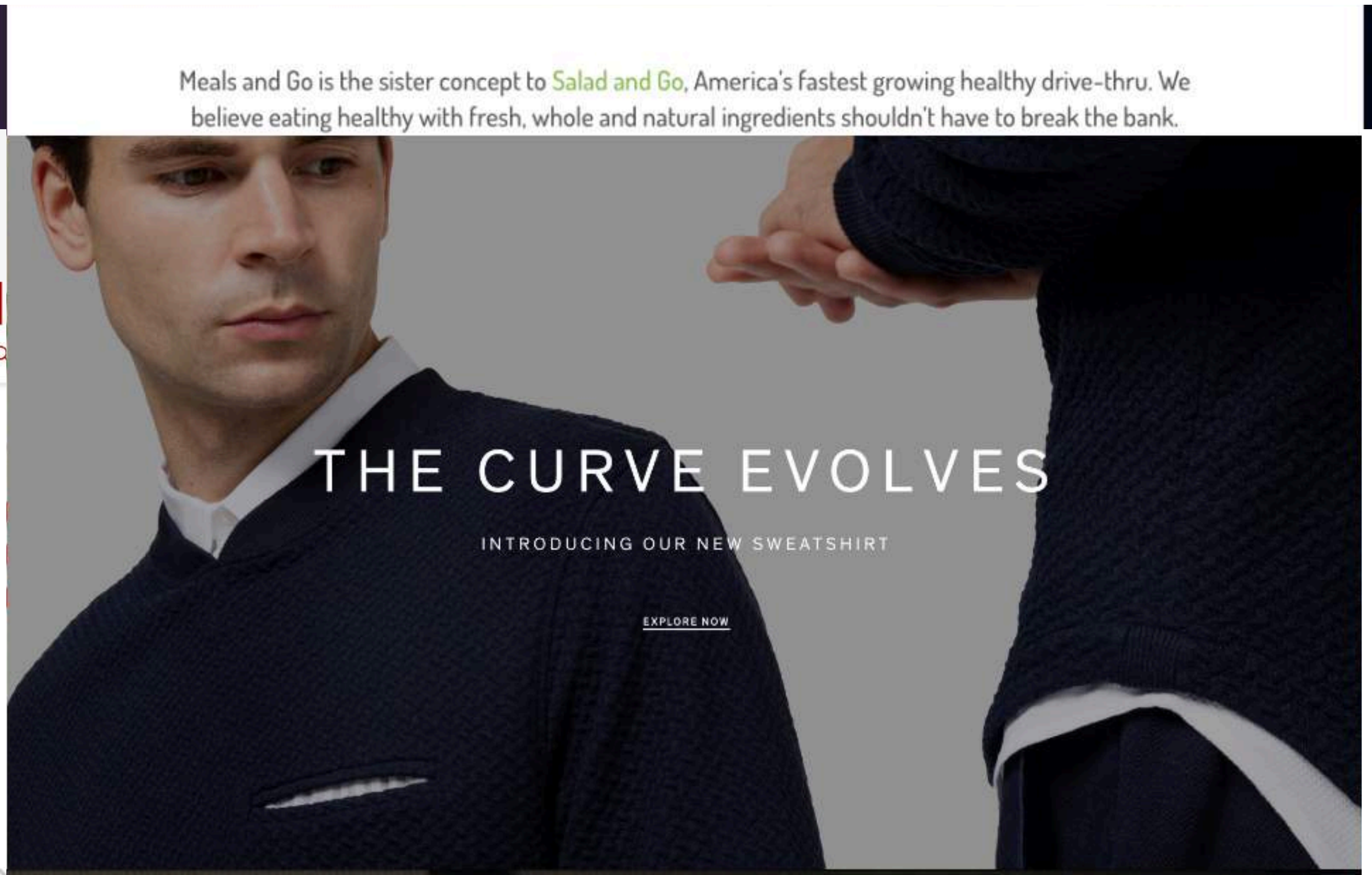
Susan B. Glasser · Friday, December 2, 2016

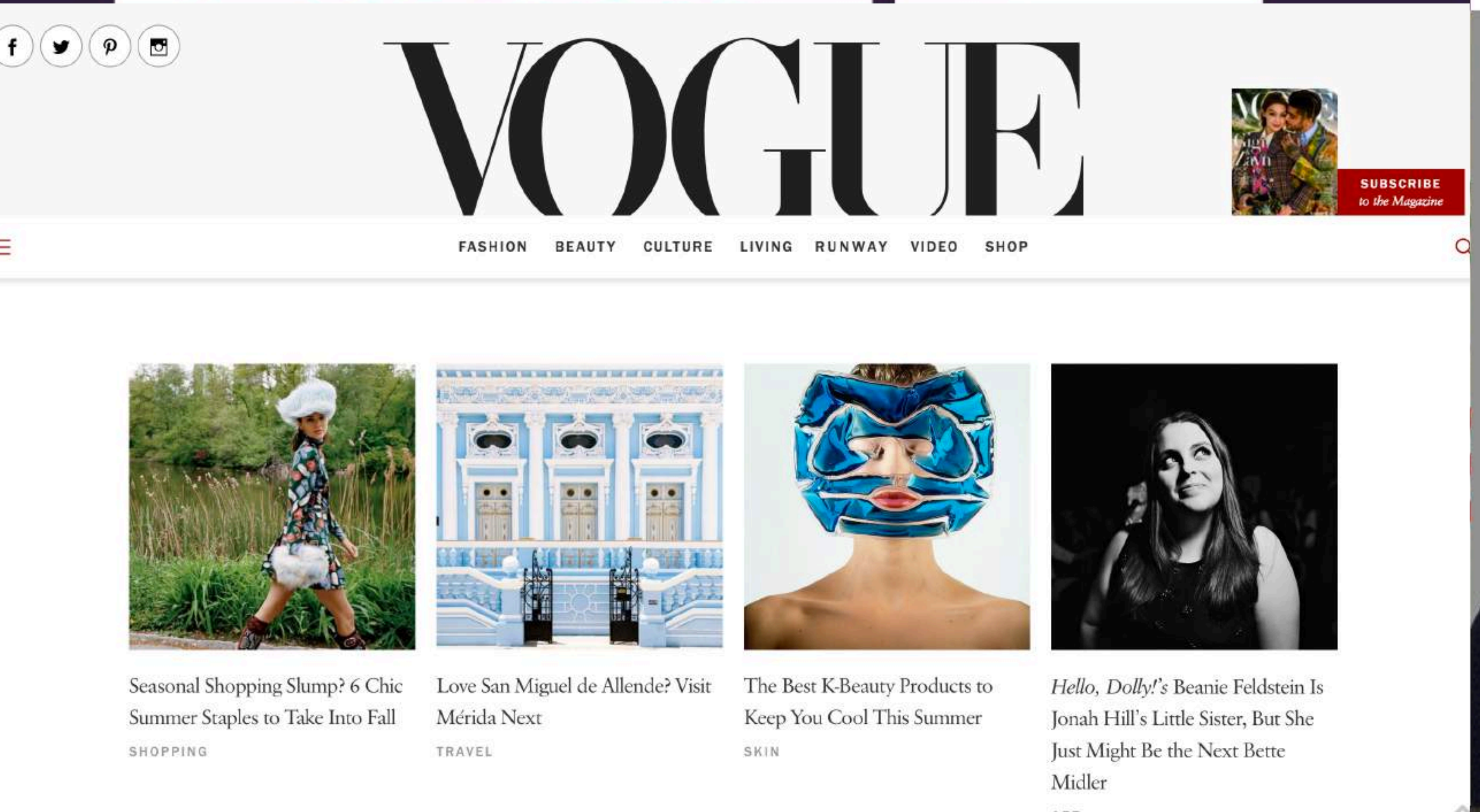
The fiscal fights of the Obama administration

Molly E. Reynolds and Philip A. Wallach · Thursday, December 8, 2016

Europe needs to take heed and reform in wake of Italy, Austria outcomes

Theodore Pelagidis · Tuesday, December 6, 2016


Meals and Go is the sister concept to Salad and Go, America's fastest growing healthy drive-thru. We believe eating healthy with fresh, whole and natural ingredients shouldn't have to break the bank.



Seasonal Shopping Slump? 6 Chic Summer Staples to Take Into Fall

SHOPPING

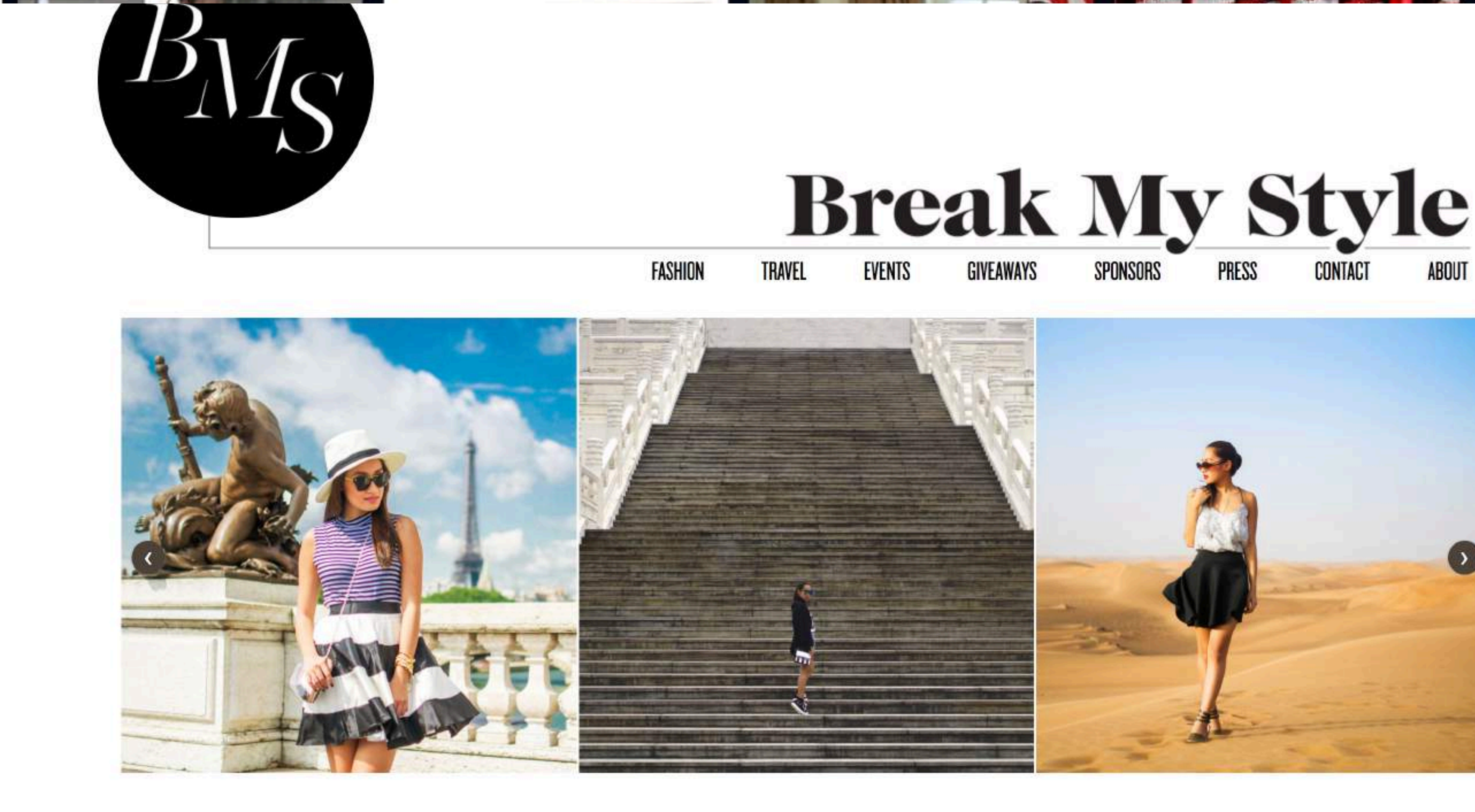
Love San Miguel de Allende? Visit Mérida Next

TRAVEL

The Best K-Beauty Products to Keep You Cool This Summer

SKIN

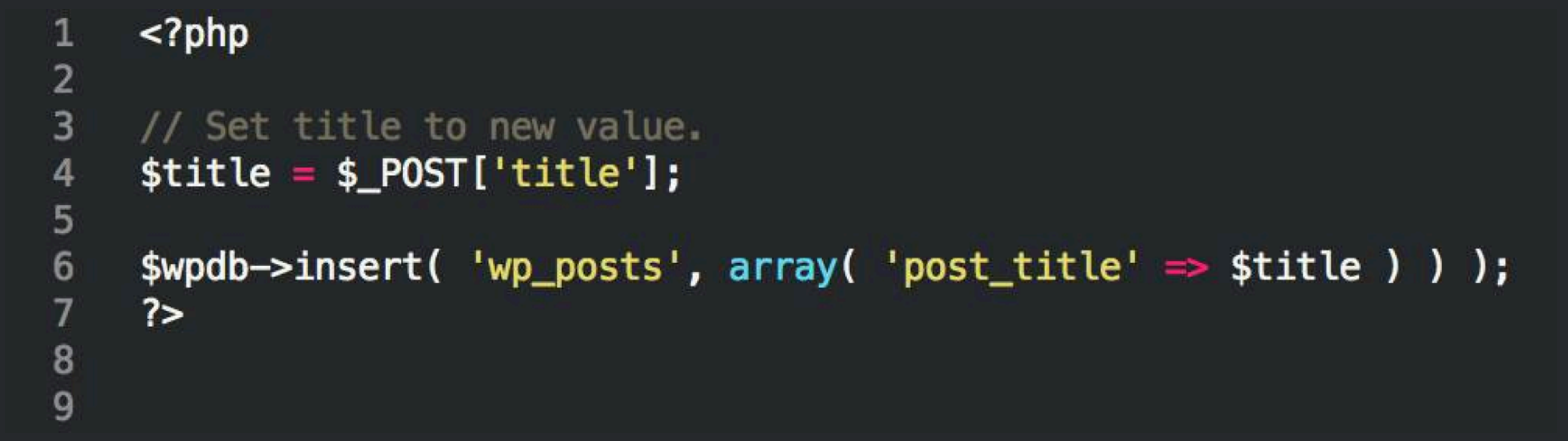
Hello, Dolly!'s Beanie Feldstein Is Jonah Hill's Little Sister, But She Just Might Be the Next Bette Midler



Security.

Sanitization & Escaping

// Saving



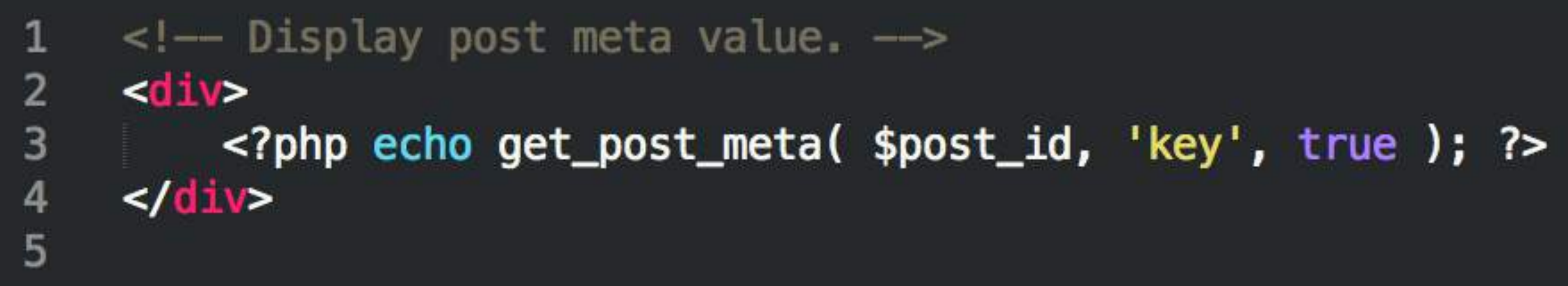
```php
<?php

// Set title to new value.
$title = $_POST['title'];

$wpdb->insert( 'wp_posts', array( 'post_title' => $title ) );
?>


```

// Output



```html
<!-- Display post meta value. -->
<div>
	<?php echo get_post_meta( $post_id, 'key', true ); ?>
</div>

```

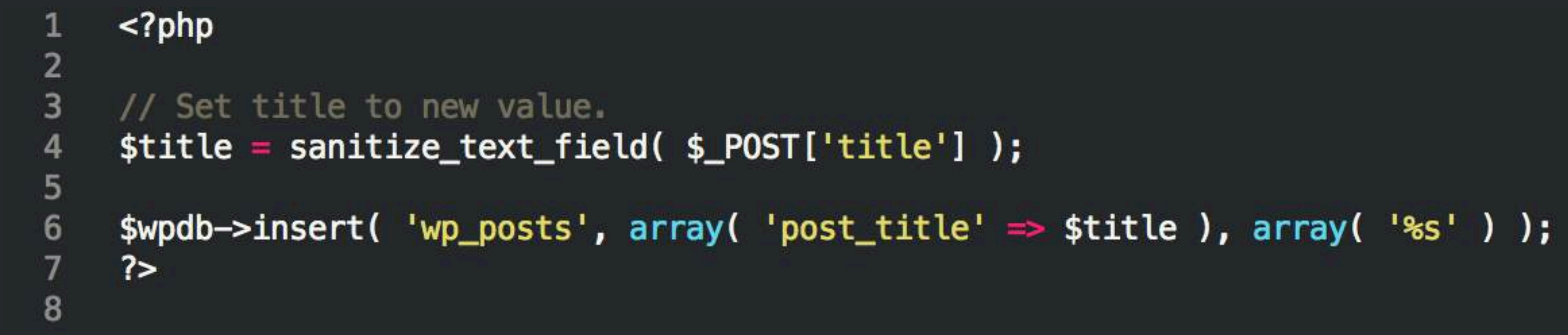
Sanitization WordPress API

- sanitize_text_field
- sanitize_email
- sanitize_key
- absint
- $wpdb->prepare()

Escaping WordPress API

- esc_html
- esc_textarea
- esc_attr
- esc_url
- wp_kses_post
- wp_kses

// Saving



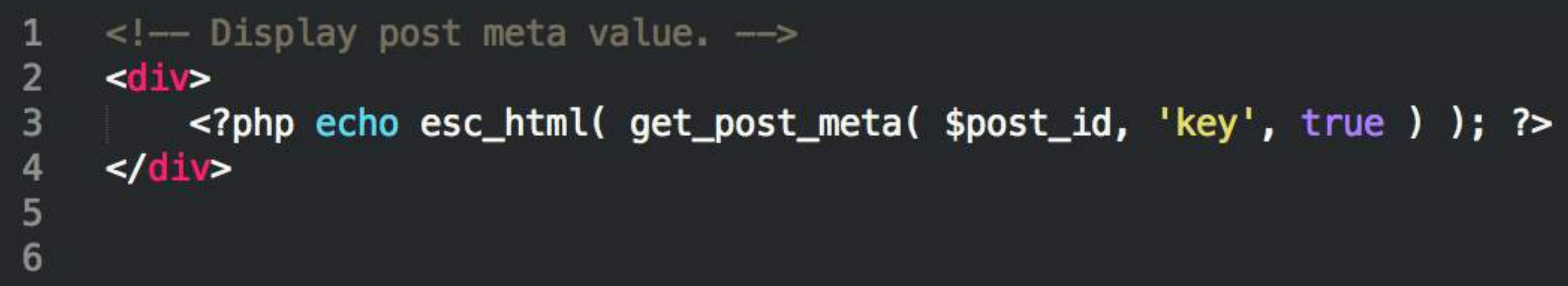
```
<?php

// Set title to new value.
$title = sanitize_text_field( $_POST['title'] );

$wpdb->insert( 'wp_posts', array( 'post_title' => $title ), array( '%s' ) );
?>

```

// Output



```
<!-- Display post meta value. -->
<div>
    <?php echo esc_html( get_post_meta( $post_id, 'key', true ) ); ?>
</div>


```

Escaping WordPress API

- codex.wordpress.org/Data_Validation
- developer.wordpress.org/themes/theme-security/data-sanitization-escaping/
- developer.wordpress.org/plugins/security/

Theme Handbook

CHAPTERS

- Getting Started
- Theme Basics
- Template Files Section
- Theme Functionality
- Theme Options – The Customizer API
- Theme Security
  - Data Sanitization/Escaping
  - Data Validation
  - Using Nonces
  - Common Vulnerabilities
- Theme Privacy
- Advanced Theme Topics
- Releasing Your Theme
- References
- Credits

Browse: Home / Theme Handbook / Theme Security / Data Sanitization/Escaping

Data Sanitization/Escaping

Sanitization: Securing Input

Sanitization is the process of cleaning or filtering your input data. Whether the data is from a user or an API or web service, you use sanitizing when you don't know what to expect or you don't want to be strict with data validation.

The easiest way to sanitize data is with built-in WordPress functions.

The `sanitize_*()` series of helper functions provide an effective way to ensure you're ending up with safe data, and they require minimal effort on your part:

- sanitize_email()
- sanitize_file_name()
- sanitize_html_class()
- sanitize_key()
- sanitize_meta()
- sanitize_mime_type()
- sanitize_option()
- sanitize_sql_orderby()
- sanitize_text_field()
- sanitize_title()
- sanitize_title_for_query()

TOPICS

Sanitization: Securing Input
- Example -Simple Input Field

Escaping: Securing Output
- Escaping with Localization
- Custom Escaping

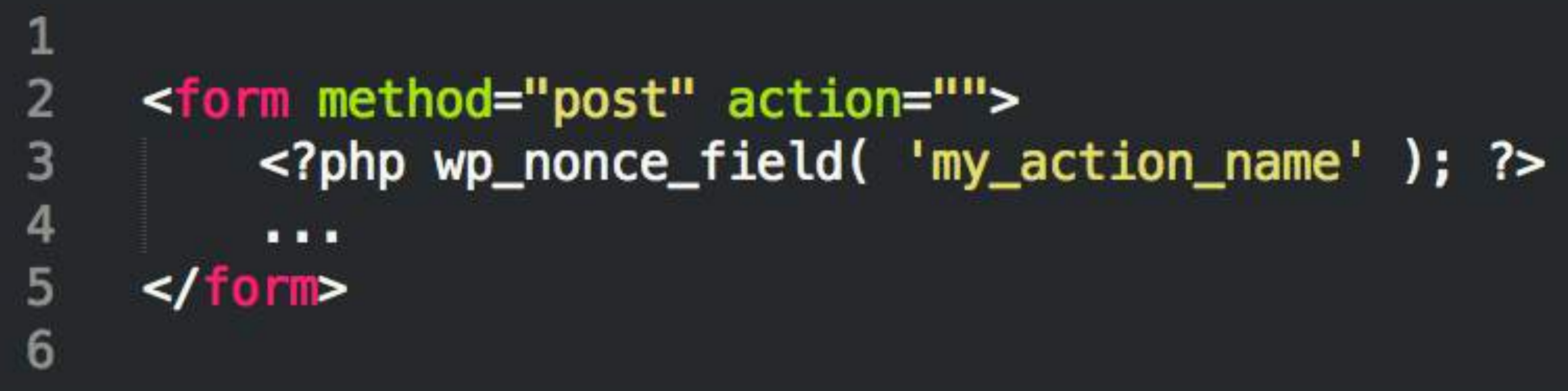
Database Escaping
- Selecting Data
- Inserting and Updating Data
- Like Statements

Nonce

Nonce

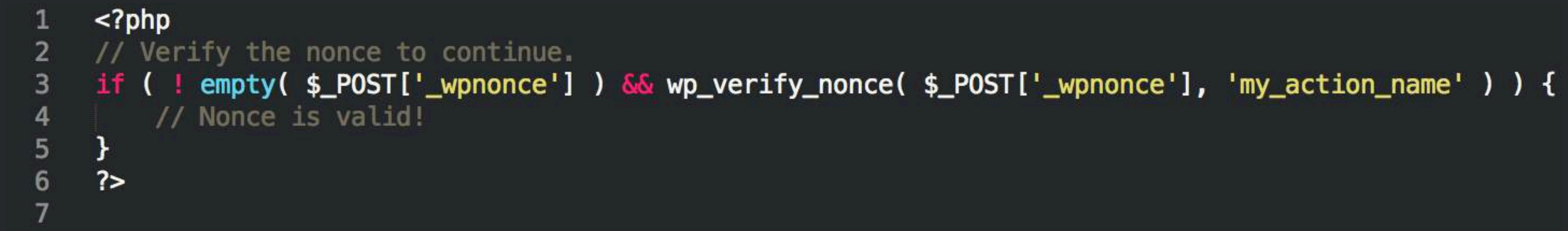
> *A cryptographic token tied to a specific action, user, and window of time.*

// Form



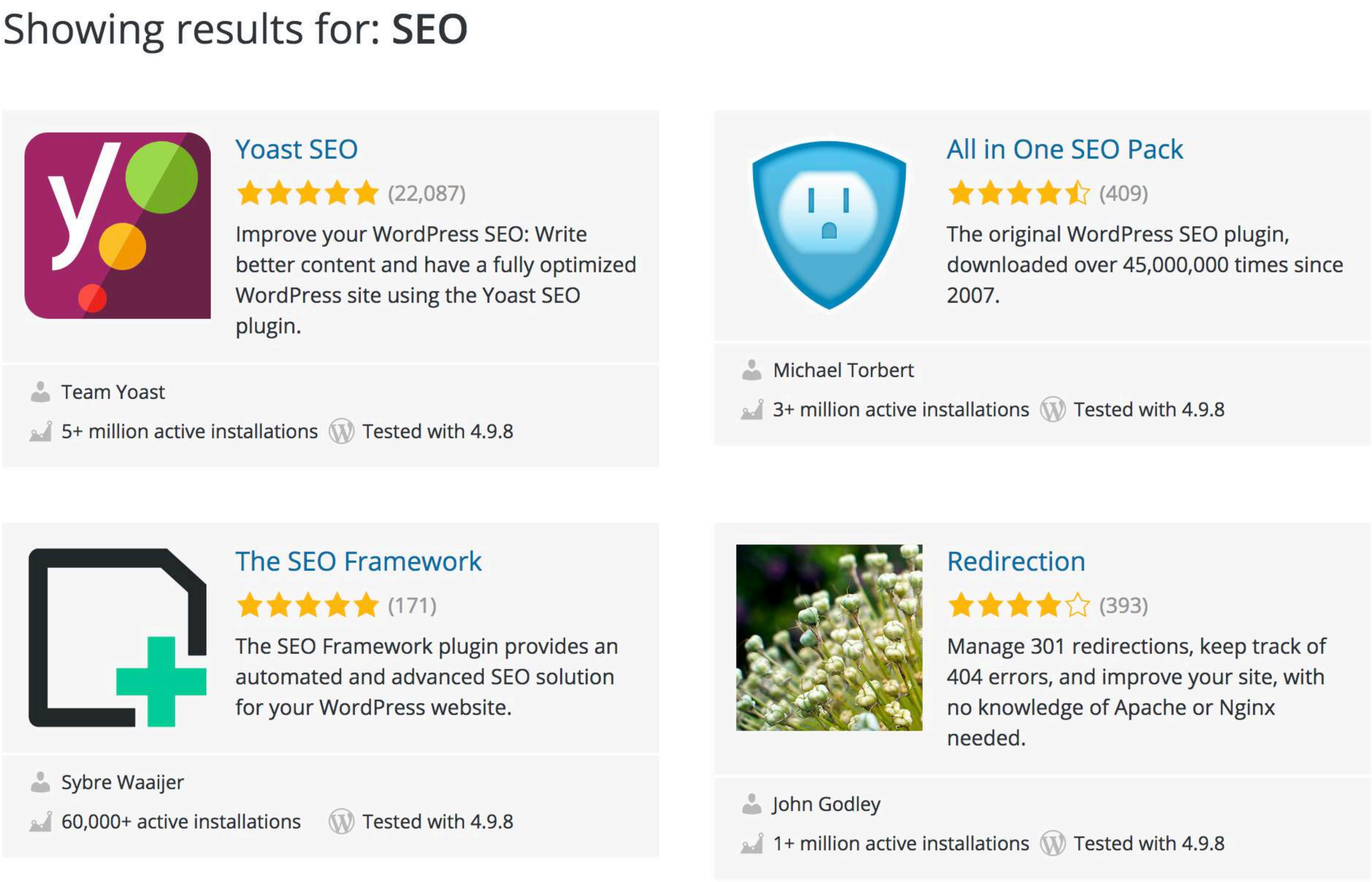
```
<form method="post" action="">
    <?php wp_nonce_field( 'my_action_name' ); ?>
    ...
</form>
```

// Process



```
<?php
// Verify the nonce to continue.
if ( ! empty( $_POST['_wpnonce'] ) && wp_verify_nonce( $_POST['_wpnonce'], 'my_action_name' ) ) {
    // Nonce is valid!
}
?>
```

Plugin Review & Moderation



Showing results for: **SEO**

Yoast SEO

★★★★★ (22,087)

Improve your WordPress SEO: Write better content and have a fully optimized WordPress site using the Yoast SEO plugin.

Team Yoast

5+ million active installations Tested with 4.9.8

All in One SEO Pack

★★★★⯪ (409)

The original WordPress SEO plugin, downloaded over 45,000,000 times since 2007.

Michael Torbert

3+ million active installations Tested with 4.9.8

The SEO Framework

★★★★★ (171)

The SEO Framework plugin provides an automated and advanced SEO solution for your WordPress website.

Sybre Waaijer

60,000+ active installations Tested with 4.9.8

Redirection

★★★★☆ (393)

Manage 301 redirections, keep track of 404 errors, and improve your site, with no knowledge of Apache or Nginx needed.

John Godley

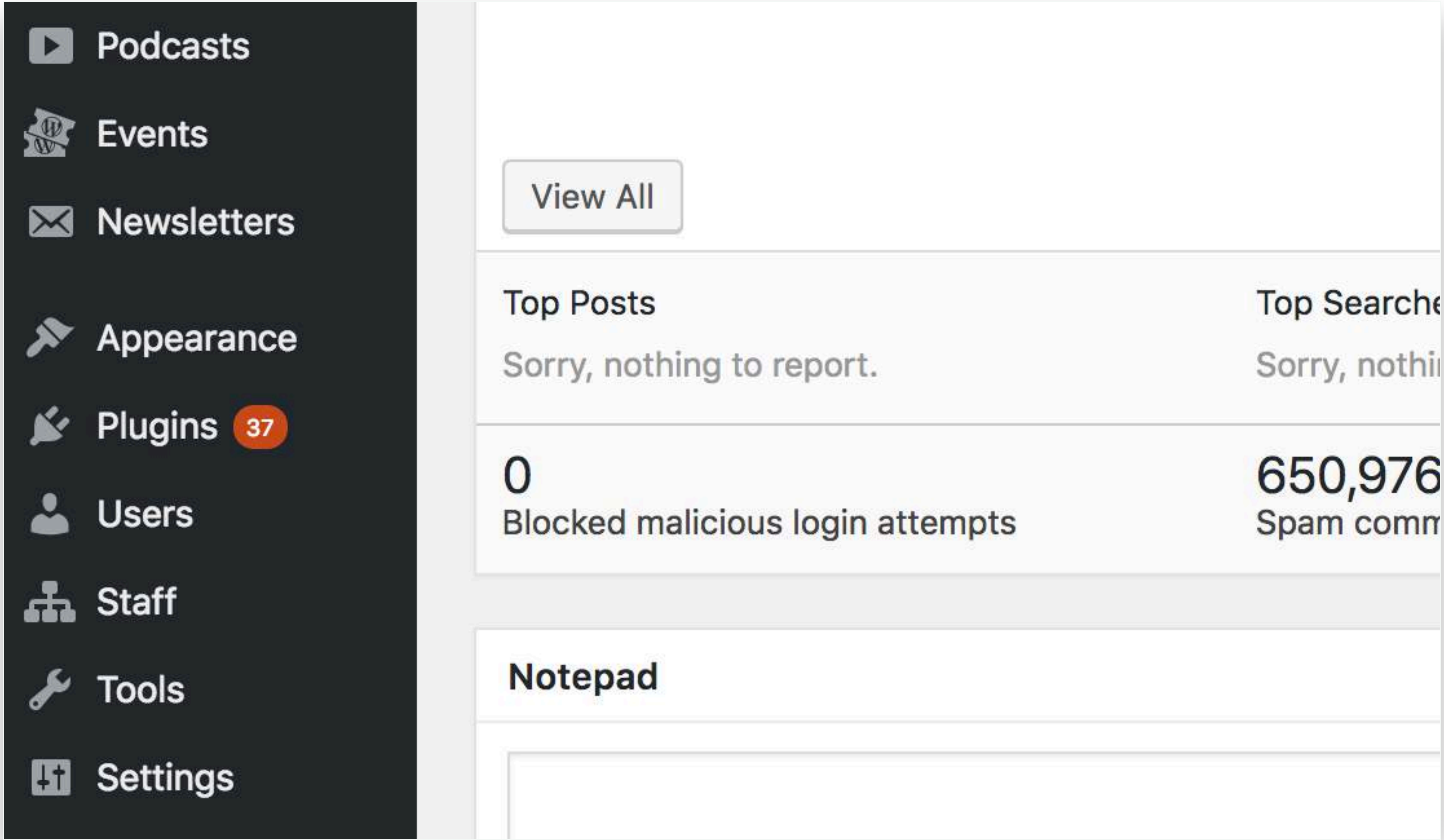
1+ million active installations Tested with 4.9.8

Plugin Review & Moderation

> *More plugins,*
> *the more vulnerable*
> *a site becomes*

Keep a list of personally/group/company **approved** plugins.

Be Updated!



Top Posts

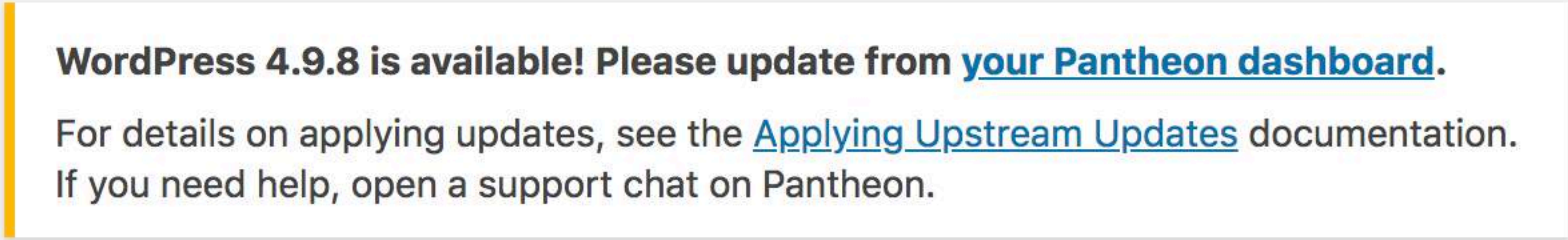
Sorry, nothing to report.

Top Searche

Sorry, nothi

0
Blocked malicious login attempts

650,976
Spam comm



WordPress 4.9.8 is available! Please update from your Pantheon dashboard.

For details on applying updates, see the Applying Upstream Updates documentation.
If you need help, open a support chat on Pantheon.

Tools & Technologies

- PHP Code Sniffer
- WordPress Coding Standards

```
➜ pure-chat-old
```

SSH & SFTP

DO **NOT** FTP!

SSH

Secure Socket Shell or
Secure Shell

SFTP

Secure File Transfer

Protocol

Contact your hosting
or Systems guy!

Performance.

Caching

> *the act of storing computed data somewhere much accessible for later use.*

- Expensive database queries
- Remote or 3rd party API requests

Object Cache

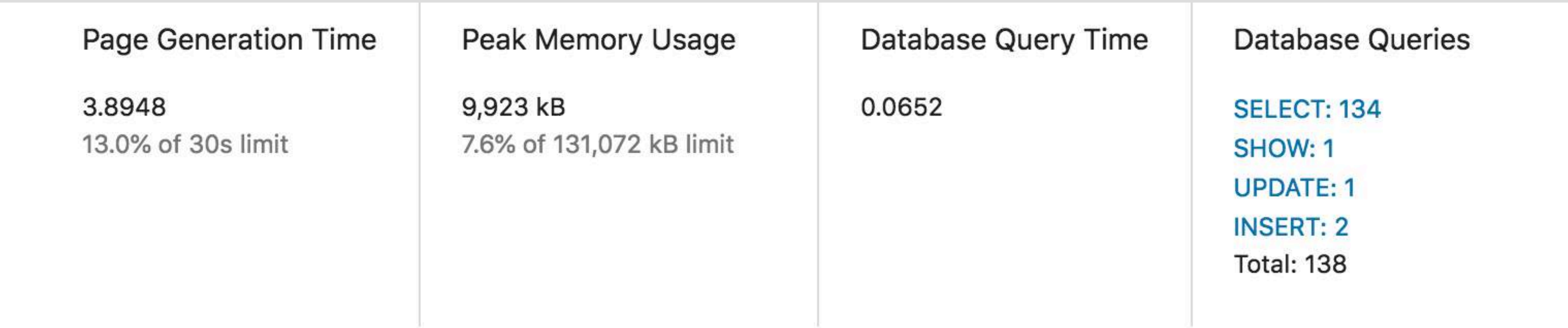
- WordPress API for caching data
- Non-persistent
- Persists with the use of:
    - Memcached
    - Redis

Caching

Transients API

Storing cached data in the options table in your database

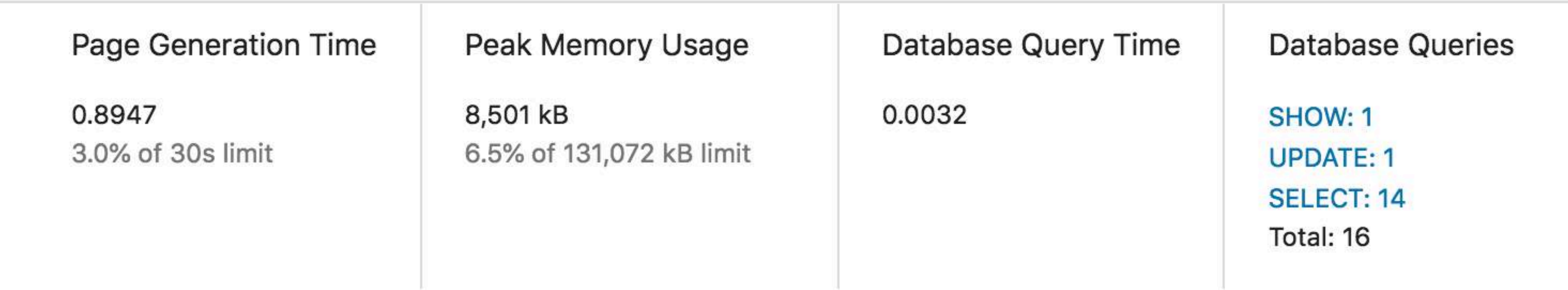
No Cache



Page Generation Time	Peak Memory Usage	Database Query Time	Database Queries

3.8948
13.0% of 30s limit
	9,923 kB
	7.6% of 131,072 kB limit
		0.0652	SELECT: 134
			SHOW: 1
			UPDATE: 1
			INSERT: 2
			Total: 138

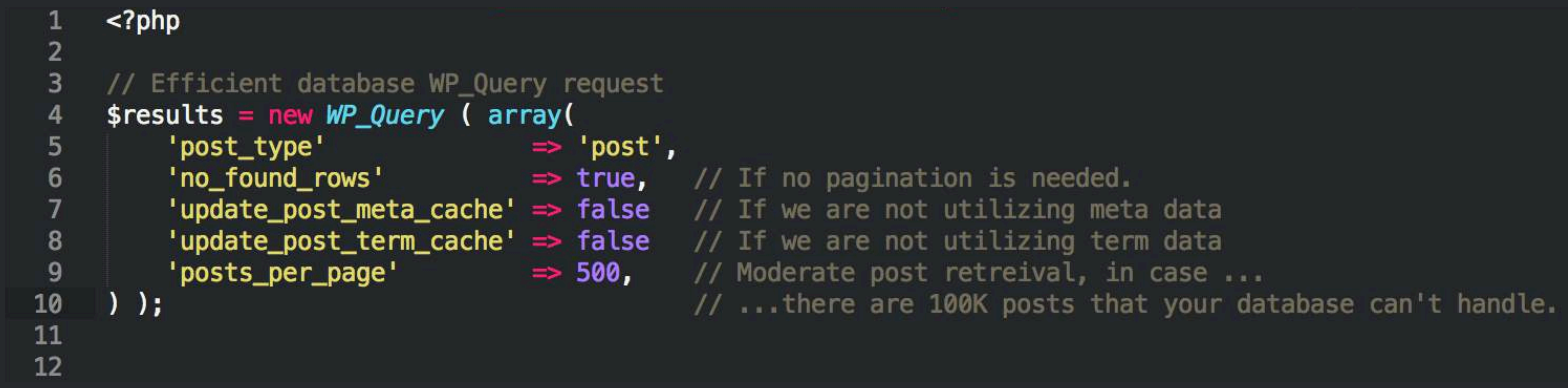
Object Cache



Page Generation Time	Peak Memory Usage	Database Query Time	Database Queries

0.8947
3.0% of 30s limit
	8,501 kB
	6.5% of 131,072 kB limit
		0.0032	SHOW: 1
			UPDATE: 1
			SELECT: 14
			Total: 16

Efficient Database Queries



```
<?php

// Efficient database WP_Query request
$results = new WP_Query ( array(
    'post_type'              => 'post',
    'no_found_rows'          => true,   // If no pagination is needed.
    'update_post_meta_cache' => false   // If we are not utilizing meta data
    'update_post_term_cache' => false   // If we are not utilizing term data
    'posts_per_page'         => 500,    // Moderate post retreival, in case ...
) );                                    // ...there are 100K posts that your database can't handle.
```

Avoid direct database query

Accessibility.

Semantics

Semantics

- header
- nav
- footer
- article
- headings (h1-h6)
- label / input

Hello ‘Aria’

ARIA —
Accessible Rich Internet Applications

Accessible Rich Internet Applications (ARIA)

> *Set of attributes that define ways to make Web content and Web applications more accessible to people with disabilities*

Accessible Rich Internet Applications (ARIA)

- States & Properties
  - aria-hidden
  - aria-required
  - aria-label
  - aria-haspopup

- Landmark Roles
  - main
  - navigation
  - banner
  - contentinfo
  - tab
  - button

Responsive
Web Design (RWD)

Responsive Web Design

- Mobile
- SEO ranking

Tools

Tools

- pa11y (terminal/CI) / koa11y (GUI)
- Chrome lighthouse
- Firefox Accessibility Inspector
  https://developer.mozilla.org/en-US/docs/Tools/Accessibility_inspector
- W3C Markup Validation Service
  https://validator.w3.org/

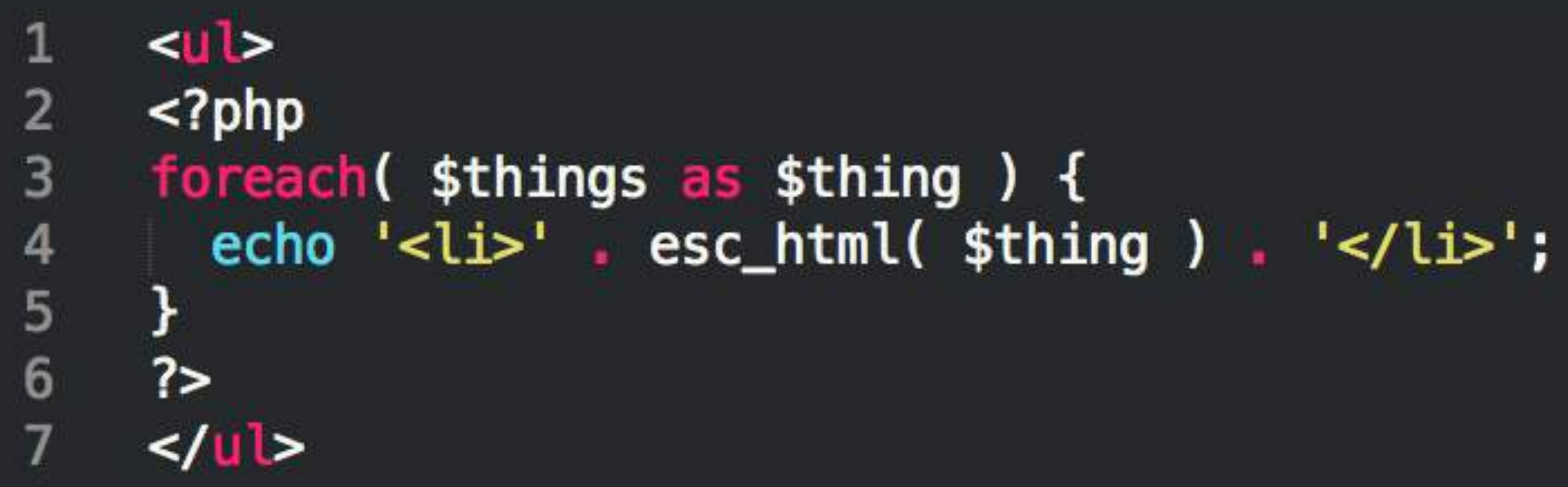
Collaboration.

Optimize Readability

Optimize Readability

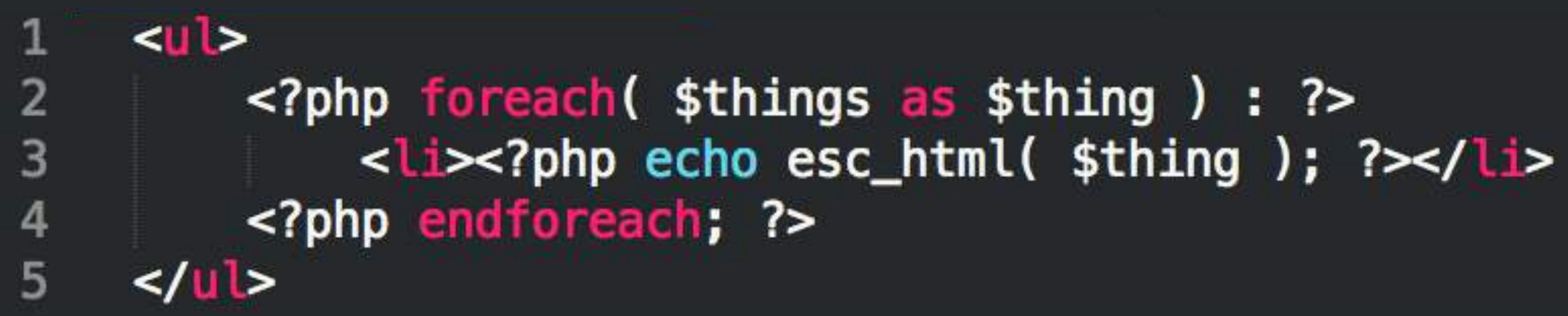
- Use **tabs** for indentation at the beginning of the line, **spaces** for midline alignment
- Keep **PHP blocks** to a minimum inside markup
- Use **colon** syntax for PHP loops and conditionals in templates

// Bad



```
<ul>
<?php
foreach( $things as $thing ) {
  echo '<li>' . esc_html( $thing ) . '</li>';
}
?>
</ul>
```

// Good



```
<ul>
    <?php foreach( $things as $thing ) : ?>
        <li><?php echo esc_html( $thing ); ?></li>
    <?php endforeach; ?>
</ul>
```

functions.php
page.php
content-audio.php
content-sample.php

```
 *
 * @link https://codex.wordpress.org/Template_Hierarchy
 *
 * @package WordPress
 * @subpackage Sample_Theme
 * @since 1.0
 * @version 1.2
 */

?>

<article id="post-<?php the_ID(); ?>" <?php post_class(); ?>>
    <header class="entry-header">
        <?php
        if ( 'post' === get_post_type() ) {
            echo '<div class="entry-meta">';
                if ( is_single() ) {
                    my_theme_posted_on();
                } else {
                    echo my_theme_time_link();
                    my_theme_edit_link();
                };
            echo '</div><!-- .entry-meta -->';
        };

        if ( is_single() ) {
            the_title( '<h1 class="entry-title">', '</h1>' );
        } elseif ( is_front_page() && is_home() ) {
            echo get_title();
        } else {
            echo get_title();
        }
        ?>
    </header><!-- .entry-header -->

    <?php if ( '' !== get_the_post_thumbnail() && ! is_single() ) : ?>
        <div class="post-thumbnail">
            <a href="<?php the_permalink(); ?>">
                <?php the_post_thumbnail( 'my-theme-featured-image' ); ?>
            </a>
        </div><!-- .post-thumbnail -->
    <?php endif; ?>

    <div class="entry-content">
```

Version Control

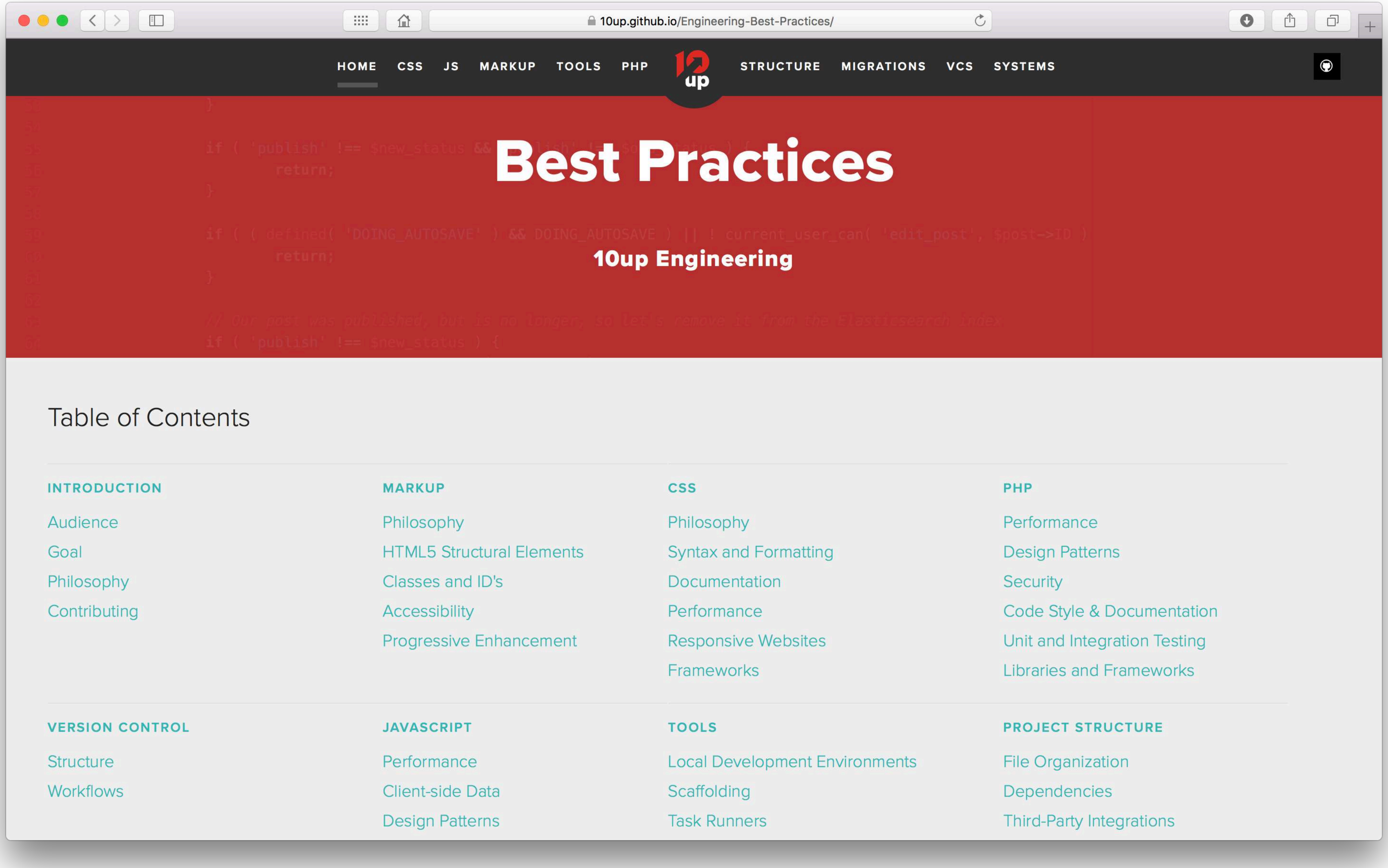
Version Control

- Github
- Bitbucket
- GitLab
- Beanstalk

Recommended Reading…

WordPress Coding Standards

- make.wordpress.org/core/handbook/best-practices/coding-standards/
- developer.wordpress.org



Best Practices

10up Engineering

Table of Contents

INTRODUCTION

Audience
Goal
Philosophy
Contributing

MARKUP

Philosophy
HTML5 Structural Elements
Classes and ID's
Accessibility
Progressive Enhancement

CSS

Philosophy
Syntax and Formatting
Documentation
Performance
Responsive Websites
Frameworks

PHP

Performance
Design Patterns
Security
Code Style & Documentation
Unit and Integration Testing
Libraries and Frameworks

VERSION CONTROL

Structure
Workflows

JAVASCRIPT

Performance
Client-side Data
Design Patterns

TOOLS

Local Development Environments
Scaffolding
Task Runners

PROJECT STRUCTURE

File Organization
Dependencies
Third-Party Integrations

Performant

Secured

Accessible

Teamwork

Thanks!

- Dreb

dreb.bits@10up.com