Lessons from WordPress
VIP
Andrew Gray

Partner / CTO
Tayloe Gray

Andrew@tayloegray.com

www.tayloegray.com

Facebook.com/TayloeGrayAgency
What is WordPress VIP

- Provided by Automatic
- Private Version of Wordpress.com
- Optimized plugins and functions
- Automatic Staff Review Of All Code Commits (via SVN)
- Unlimited Traffic at a flat monthly fee
The Site
## The Traffic (one month)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions</td>
<td>6,907,701</td>
</tr>
<tr>
<td>Users</td>
<td>2,411,578</td>
</tr>
<tr>
<td>Pageviews</td>
<td>17,765,632</td>
</tr>
<tr>
<td>Pages / Session</td>
<td>2.57</td>
</tr>
<tr>
<td>Avg. Session Duration</td>
<td>00:05:31</td>
</tr>
<tr>
<td>Bounce Rate</td>
<td>51.68%</td>
</tr>
<tr>
<td>% New Sessions</td>
<td>30.64%</td>
</tr>
</tbody>
</table>
Dev on Quickstart
Staging
VIP
Quickstart

VIP Quickstart is a local development environment for WordPress.com VIP developers. It provides developers with an environment that closely mirrors WordPress.com.

- Local
  - VirtualBox
  - Vagrant
  - Git

- Public Server
  - Tested with a host running Ubuntu 12.04
  - Git
  - Puppet
My Pain is Your Gain

What doesn’t kill you, makes you stronger
Hi,

I am about to deploy, but I have a few suggestions were the code can be improved in terms of readability:

- includes/feeds/daily-feed.php:
  - 96, 97: I would suggest simply calling `current_time('timestamp')` – it would make the code clearer.
  - 99, 100: true/false should be lowercase
  - 101: `$article_flag === 'deal-expired'` should be reversed: 'deal-expired' === `$article_flag`

I suggest these improvements will be done, and then I will deploy that change.

All the best,
Gudmundur
Coding for Others to Review

- Removing Commented-out code
- Write for a non-related developer to review
Hi Andrew,

in line 398 of TEMPLATE-CONTACT-V3.PHP$_SERVER['HTTP_USER_AGENT'] is an end user provided variable, So it needs to be escaped on output.

Thanks!

Stéphane Boisvert | Support Team Lead | WordPress.com VIP
Escape Outputs / Sanitize Inputs

- **Guiding Principles**
  - Never trust user input.
  - Escape as late as possible.
  - Escape everything from untrusted sources (like databases and users), third-parties (like Twitter), etc.
  - Never assume anything.
  - Never trust user input.
  - Sanitation is okay, but validation/rejection is better.
  - Never trust user input.
Sanitize and Escape

- 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()
- sanitize_title_with_dashes()
- sanitize_user()
- intval()
- wp_kses()
- wp_kses()
- esc_textarea()
- esc_attr()
- esc_js()
- esc_url()
- validate_file()
Deploy Via SVN / Git

- Code review and testing prior to deployment
- VIP Deployments happen when code gets approved, not when scheduled
- Coding with settings, All updates must be written into code, or done after launch.
Hi Andrew,

static/inc/cpt/cpt-megamenu.php line 745, 756, 763, 770, 777 are missing escaping ... please also fix the same problem in the various callback functions that use printf to output. All of them need to escape.

It might take a while to review/verify the javascript you've committed -- it's over 15,000 lines, which is larger than we usually see in the live deploy queue. Most of it seems to be standard libraries which should be easy to verify and approve, but there might be a brief delay.

Thanks,

Matt

WordPress.com VIP
If it is important, code it yourself

- VIP supports / allows limited number of plugins
- Skip plugins for basic functionality such as Custom Post Types
- Many plugins are overkill
Stuff they look for

- Uncached Functions
- Unprefixed Functions / Namespaces
  - theme_name_function_name()
- Failing to check current_user_can()
- Arbitrary JavaScript and CSS stored in options or meta
- Waiting on Remote API calls
- Order By Rand / No LIMIT queries
- Skipping the cache with query vars
- *_meta as a hit counters