Drupal 7
Website Audit

example.com

We performed an in-depth site audit in order to learn about the current state of the site (ie. how much pending maintenance needs to be performed) and to estimate the level of effort necessary to support and maintain the site going forward.

This includes:

- Checking the version of Drupal core and any contrib modules, to see if any security updates need to be performed, or if any unsupported, uncommon or high-risk modules are in use
- Looking for signs that the site has been hacked, or has any insecure configurations that would make it easier to hack
- Evaluating the complexity of the site to determine how difficult it is to make changes (without breaking anything or causing additional problems)
- Reviewing any custom modules or themes to see if they follow best practices, and determining if they'd require an additional bucket of hours in order to maintain
- Searching for anything else that might make supporting or maintaining the site harder

All of the problems identified in this report are things that we'd be happy to fix as part of the maintenance plan if the customer chooses to work with us!

However, we include recommendations that you (or another vendor) could implement to make the site more easily maintainable, even if they don't decide to work with us.

Drupal core, contrib modules and themes

The site runs **Drupal 7.41** which is the latest version!

There are **157 modules enabled** (which is higher than average), but there are **no modules with pending security updates!**

The site uses one uncommon modules:

- guzzle

While these aren't necessarily bad, uncommon modules present a potentially higher risk with regard to long-term maintenance. They are more likely to contain bugs or security issues (and it's more likely that those security issues will never be found, because fewer people are looking for them!).

Security

We weren't able to find any obvious signs that the site has been hacked!

In the logs there were numerous failed login attempts from a single IP that could represent an attempt to brute force guess passwords:

- 91.200.12.22

We also audit site configuration for settings that can make your site less secure. Fortunately, we didn't find anything! I think this might be the first site audit report where we had no configuration recommendations. :-)

Custom modules and themes

There are no custom modules!

There is one custom theme 'mytheme' which has no base theme. It is moderately complex, made up of 25 templates, 312 lines of PHP, 1652 lines of Javascript, 4097 lines of CSS. There are no database queries in the theme (a good thing!) and while the code's a little messy, there didn't appear to be any obvious problems.

The custom theme is the only thing identified here that significantly increases the maintenance burden of this site, and even that, is not by much. :-)

Conclusion

While there are a few pending maintenance tasks related to security, this site appears to be quite well maintained and have a relatively low maintenance burden!

Based on our audit, **we'd recommend either the "Standard" plan ($625/mo) or "Basic" plan ($125/mo)**. Both plans include:

- Making security fixes
- Fixing bugs that prevent users from performing critical use-cases
- Getting your site back online in case of an outage
- Remediation if your site has been hacked

Additionally, the "Standard" plan includes:

- Performing basic one-off maintenance and support tasks on request
- We'll work with your existing hosting provider (the "Basic" plan requires moving to Patheon or our Drupal-optimized shared hosting platform)

Please let us know if you have any questions!