Contents

1. Introduction

An audit order for the website {REDACTED URL} was received on 12.4.2024 at 15:46 from the address {REDACTED EMAIL ADDRESS}.

The results below are the result of investigating the current website, visible code, and speed testing tools to get a basic overview of the security and technical quality of the website. No active scanning methods were used during this audit.

The audit was completed by Lisa-Marie Karvonen.

The audit was conducted following guidelines set out in the ISO 19011:2018 Guidelines for auditing management systems standard.

2. Risk Overview

This table shows the number of issues in each category. The table is also coded to severity level whether it's HIGH risk, MEDIUM risk, or LOW risk.

Risks			
Type	High	Medium	Low
Security	11	3	2
Privacy	-	1	1
SEO/Speed	-	2	2
Usability	-	1	1

3. Findings

3.1 Basic Information

Nameservers	{REDACTED NAMESERVER} {REDACTED NAMESERVER}
Hosting	IP: {REDACTED IP} {REDACTED URL}
Server	Apache
DB	MySQL/MariaDB
CMS	WordPress
Theme	{REDACTED THEME NAME AND VERSION} {REDACTED CHILD THEME INFO}

3.2 Security Findings

Risk Factor	Item
High	The parent theme's latest version is 3.2.4 and the version is 2.4.8. The parent theme should be kept up to date. It's best to make small updates often, rather than update the theme infrequently so it doesn't break so easily.
High	Your server is leaking directory information and filenames from {URL REDACTED}. You need to turn off directory listing in all of your directories.
High	WordPress version is displayed as 5.8.9 which was released on 30th January 2024. The current version is 6.5.2. It's recommended to keep the WP core up to date as soon as new releases are available.
High	The server headers do not protect your site at all. You can see the results here: {URL REDACTED}

High	Contact Form 7 version is 5.4.2 and the latest is 5.9.3. Recommended to keep all plugins up to date especially plugins that handle user input (form plugins, e-commerce solutions etc).
High	Cookie Law Info plugin is out of date. Installed version is 2.0.6 but latest is 3.2.1. Recommended to keep all plugins up to date.
High	Js_composer plugin is likely out of date. Showing version 6.7.0, latest version is 7.5. Passive detection used.
High	LayerSlider plugin is likely out of date. HTML meta generator tags in the homepage show Layerslider 6.11.9. LayerSlider latest version is 7.10.1. LayerSlider is a premium plugin, it's worth paying for a license and keeping it up to date.
High	WP-Rocket is showing as version 3.7.2. The latest version is 3.15.10. This should be kept up to date as the other plugins.
High	With WordPress core and multiple plugins showing as outdated, there's a high likelihood of other plugins that are not found using passive scanning as being out of date. It's recommended to update all plugins, core and themes.
High	The login is not secured. When trying the username 'admin', the site tells me that there isn't a user called admin and to try using my email address. Ideally, WordPress shouldn't reveal anything and in the best cases should block a user who tries to use an obvious username such as admin. Wordfence is a good plugin to protect login and also has a lot of other features.
Medium	There is a data leakage in the code. For example, Layerslider, revslider, WP version, WP Bakery, Redux 4.3.1 etc. They are all leaking versions that give critical information to bots and attackers about where your site vulnerabilities are. This kind of leakage is common when using ready-made themes and plugins, but your site has even more leakage than usual.

Medium	Some other plugins found were massive-elements-for-wpbakery, and mpc-massive. These plugin versions couldn't be determined, but these are plugins found from a passive scan which means that there's likely to be a lot more plugins under the hood in the admin. Also, revslider is out of date. It's unlikely that your site needs two different slider plugins. Recommended to remove as many plugins as possible to reduce surface attack area. The more plugins, the more area for bots to use.
Medium	You might consider setting up WP-cron to run internally. At the moment it can be run externally {URL REDACTED}. This would improve performance.

Low	The {URL REDACTED} allows indexing access to pretty much everything. Recommended disallowing certain folders such as wp-admin. Yoast SEO would help with this but an example would be:
	
	`User-agent: *`
	`Disallow: /wp-admin/`
	`Disallow: /wp-login.php`

Low	You may wish to block access to {URL REDACTED} XML-RPC if you are not using any of the remote posting features. This tightens up security. For more information check: https://www.hostinger.com/tutorials/xmlrpc-wordpress another effective way to block it is through Cloudflare.

3.3 Privacy Findings

Risk Factor	Item
Medium	The site uses Google Fonts. Google Fonts are not fully GDPR compatible. The solution is to self-host fonts by uploading them to your server and updating the theme code. This would also help with website speed and reduce the risk of latency of the site.
Low	Possible data leakage. Your sitemap is possibly leaking usernames and names here: {URL REDACTED}. It's a good idea to shut down any automatic listing of usernames.

3.4 SEO/Speed Findings

Risk Factor	Item
Medium	GTMetrix gave your site a test result of F (testing from Canada). The loading time was 6.2 seconds.
Medium	Your site received a speed test result of B from Pingdom (testing from Germany) which is OK but could be improved. The page size was still 2.5 MB and had 88 requests and 15 of those were from domains outside of your control with the slowest one being Google Fonts. It's recommended to serve as much from your own domain as possible for speed and security.
Low	Your theme is loading a lot of different fonts from both Google Fonts and also from the theme directory. This could be cleaned up so that the site would work faster.
Low	Caching could be optimised a bit better. You have a CDN working but you may want to consider more benefits of Cloudflare's DDoS protection and speed improvements.

3.5 Usability Findings

Risk Factor	Item
Medium	The website menus do not have enough contrast with the background. The red hover on the menu makes the contrast worse.
Low	The site logo is blurry on high-res devices and when scrolling down, elements are on a white background which gives the site a choppy look. All of these visual findings are of course a matter of taste, but content that is centered, and then left justified, then centered again, can be very confusing to users. A lack of spacing between some elements, and too much space between others, can make usability hard for most users. Contrast issues mean the website is not accessible to visitors with visibility issues for example. It's recommended to simplify elements and give them space, as well as toning down some colours, to give the website a more unified feel. An example of this is shown in Attachment 2 below.

3.6 Other Findings

Risk Factor	Item
None	Your website went down during testing. It's likely that the host blocked our testing IP since the site worked from a mobile connection and from: {URL REDACTED} This is good. It means your host is at least a little proactive if someone runs scans on your website. We did not use any active scanning or pen testing on your site, but even passive scans can alert WAF's to potential issues.
None	Your site doesn't appear to save any cookies other than the Cookie Law plugin cookies which is a good thing. We tested with CookieBot scanner as well just to make sure and it looks good. A screenshot is attached as Attachment 1 below.

3.7 Attachments

Attachment 1: CookieBot Scanner results show that the site is low risk.
{IMAGE REDACTED}

Attachment 2: An example of the homepage when it gets confusing during the hero area.
{IMAGE REDACTED}

Attachment 3: GTMetrix results could be improved upon but testing was from Canada so that affects speed of course.
{IMAGE REDACTED}

4. Summary and More Information

We hope you find this audit information useful in securing your website. If you have any questions about this audit or its findings or would like us to take care of these issues for you. Please don't hesitate to contact us using the details below.

Lisa-Marie Karvonen
Website Security Specialist

050 3139531
lisa@wpensure.com