American Academy of Dental Sleep Medicine

Website: https://dentalsleep.org

Security Notes

WordPress Version 6.8.3 (Latest version: 6.9)
Update Recommended

DB Version: 10.6.24-MariaDB-cll-lve

Users

- The site has 3 users
  - aadsm@knbcomm.com
  - broberts@aadsm.org
  - website@knbcomm.com

All users have admin privileges. We highly recommend adding 2FA to the login process.

Themes

- The website uses Elementor with a Child Theme.
- There are five additional themes that are recommended for deletion to prevent access to unused code.

Your site has 7 installed themes, all up to date.

Your site has 4 inactive themes. To enhance your site's security, you should consider removing any themes you are not using. You should keep Twenty Twenty-Five, the default WordPress theme, Hello Elementor Child, your active theme, and Hello Elementor, its parent theme.

Plug Ins

Your site has 10 active plugins, all up to date.

Your site has 1 inactive plugin. Inactive plugins are tempting targets for attackers. If you are not going to use a plugin, you should consider removing it.

Installed Plugins (10)
Active (9)
Inactive (1)

Pages and Posts

Posts

- Currently, the site has no active posts, but it has 81 deleted posts that are spam.
- **Recommended**: Delete all these posts and verify all database tables for it.

Pages

- Active Pages 15
- Draft 1 Page
- Private 1 Page

WordFence Security Plug-In

The Wordfence WordPress security plugin provides free, enterprise-class protection for your website, helping prevent hacks and malware.

1. The Plugin "Piotnet Addons For Elementor" has a security vulnerability.
    a. Type: Plugin Vulnerable
    b. Issue Found January 25, 2026 12:54 am
2. WordPress core file modified: index.php
    a. **Type**: File
    b. **Issue Found** January 25, 2026 12:28 am
    c. **Priority**: High
    d. **Filename**: /home/gdmnwq314l2e/public_html/index.php
    e. **File Type**: Core
    f. **Details**: This WordPress core file has been modified and differs from the original file distributed with this version of WordPress.

Server Audit

DNS: https://dentalsleep.org/ DNS is served by GoDaddy DNS with Proxied security
NO SMTP Module found

Hosting: GoDaddy (cPanel)

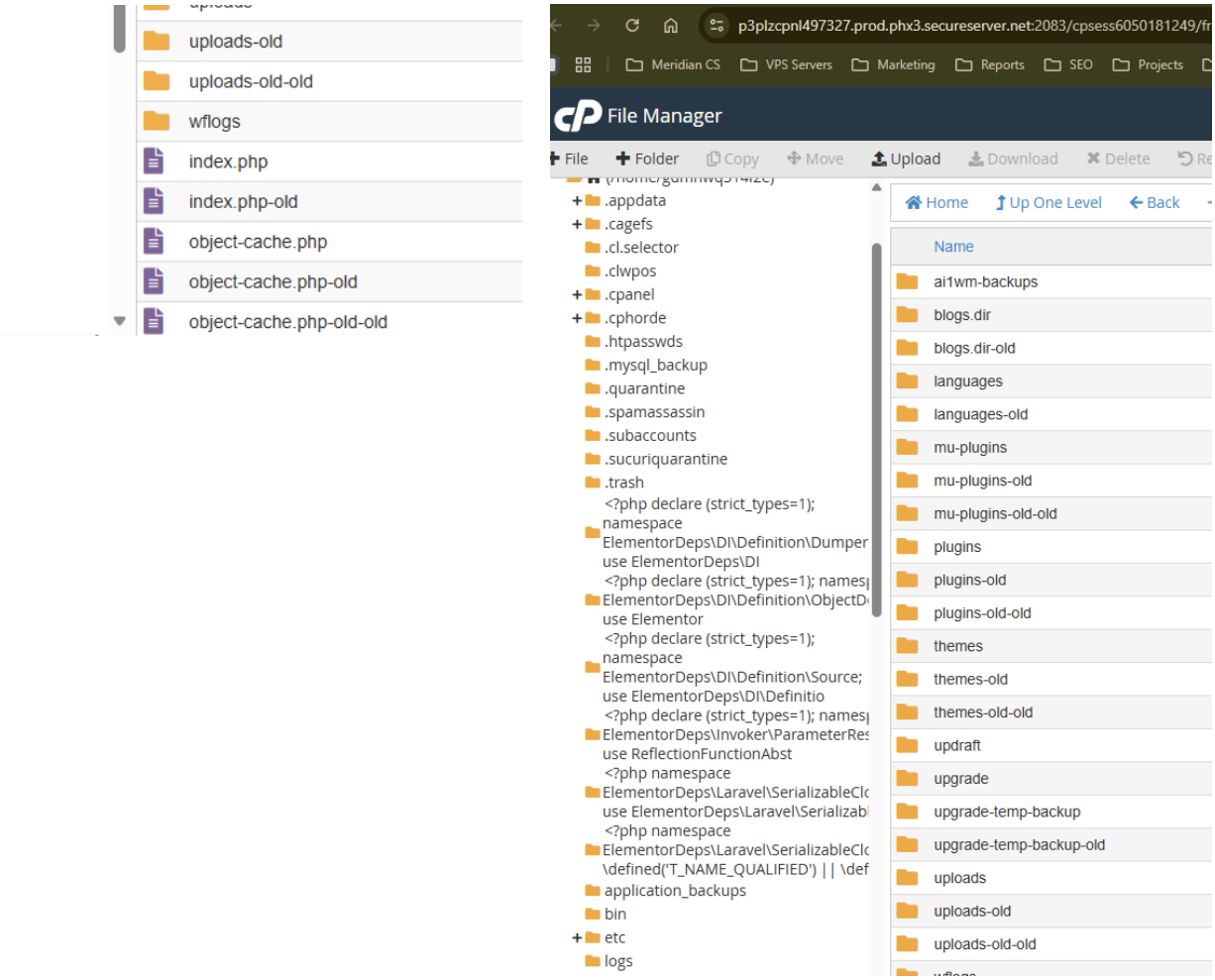
CRITICAL ISSUE: GoDaddy Hosting is still using PHP7.4.33

It looks like GoDaddy charges for Extended Support for PHP 7.4, which makes no sense. PHP should be upgraded to at least 8.3.

WordPress update available (6.9) Performance A new version of WordPress is available.
PHP is one of the programming languages used to build WordPress. Newer versions of PHP receive regular security updates and may increase your site’s performance. The minimum recommended version of PHP is 8.3.
Plugins extend your site’s functionality with features like contact forms, e-commerce, and more. That means they have deep access to your site, so it’s vital to keep them up to date. Your site has 1 plugin that needs updating. Your site has 1 inactive plugin. Inactive plugins are tempting targets for attackers. If you are not going to use a plugin, you should consider removing it.
Page cache is not detected, but the server response time is OK Performance Page cache enhances your site's speed and performance by caching and serving static pages instead of loading them every time a user visits.
Your site has 4 inactive themes. To enhance your site’s security, you should consider removing any themes you are not using. You should keep Twenty Twenty-Five, the default WordPress theme, Hello Elementor Child, your active theme, and Hello Elementor, its parent theme.

Lots of duplicate folders. WordFence was installed at some point, but later on removed.
Scanned unused PHP files. These files are recommended for removal from the server.

GoDaddy cPanel does not include security modules to scan the server.



There are many strange folders in the server's root directory.

WordPress and Server Recommendation

WordPress Recommendation

Install

- **Security**: We highly recommend installing WordFence to monitor site files and login activity. WordFence will notify you whenever a user attempts to access the site, including the time and location of that user.
- **Cache**: Page caching enhances your site's speed and performance by storing and serving static pages instead of generating a page each time a user visits. A page cache plugin was not detected.

Remove:

- Piotnet Addons For Elementor
    - This plugin is installed but not active. At this point, for security, we would like to remove anything that is not being used.
- WpCode Lite
    - This plug-in is active; however, no snippet has been used. Basically, the plug-in is not being used by the website.

Server Hosting Recommendation:

- Web application firewall (WAF)
- Distributed denial of service (DDoS) protection
- VPS server (with SFTP Access using Keys and only VPN)
- Malware protection
- PHP Update
- Limit Admin users
    - Required 2FA
- Strong Passwords
    - Weak or easily guessable passwords leave your site vulnerable to unauthorized access and expose your site to botnets. Botnets are collections of computers infected with malware and under the control of a hacker. They are the leading cause of DDoS attacks on the internet, but you can prevent your site from falling victim to them by taking the correct precautions.
- Security Audit

Backup Process Audit and Recommendation

Currently, the site uses UpdraftPlus for backups. (Good)

However, the site is set up for daily backups with a 2-day retention policy. In addition, there are no remote backups, and backups are stored only on the server.

A 2-day backup window is too short for recovery, and the backups are on the same server. If files are corrupted locally, the backups are also lost.

Proposed

1. We would like to connect our Updraft Professional account, which backs up to both a local server and a remote location simultaneously.
2. Retention Policy update to:
    a. Backup DB daily with 14 days of retention
    b. Backup server files weekly with 3-week retention