Guard Dog

Security Report
test.wpfixithosting.com

Security Score

100

This is a website security snapshot dated October 10, 2024

Great work on securing the items below_

- ✓ Site Lock is enabled to restrict access to your site
- ✓ Stop Registration is enabled to prevent unauthorized user registrations
- ✓ X-Content-Type-Options is enabled to prevent MIME type sniffing
- ✓ X-Frame-Options is enabled to protect against clickjacking
- ✓ X-XSS-Protection is enabled to help prevent cross-site scripting attacks
- ✓ Strict-Transport-Security is enabled to ensure secure connections (HTTPS)
- ✓ Referrer-Policy is enabled to control information sent in the Referer header
- ✓ Content-Security-Policy is enabled to mitigate XSS attacks
- ✓ XML-RPC is disabled to prevent certain types of attacks like brute force
- ✓ Commenting is disabled to reduce spam and malicious content
- ✓ User Enumeration is disabled to prevent attackers from discovering valid usernames
- ✓ File Editing is disabled to prevent unauthorized changes to your theme or plugin files
- ✓ REST API is disabled to reduce the attack surface for certain vulnerabilities
- ✓ WordPress Version Display is disabled to hide potential vulnerabilities
- ✓ A Custom Login URL is set to hide the login page

Virus Scan Results

You can view a full virus scan result for this site by clicking the link View Scan Results

WordPress Enviroment

Keeping WordPress core updated is crucial for maintaining security, performance, and compatibility.

✓ WordPress is up to date running on the current version **6.6.2**

Installed Plugins

Inactive and outdated plugins can pose significant security risks and vulnerabilities, potentially exposing your WordPress site to attacks. Only up to date active plugins should be on your site.

✓ Active Plugins

- Anti-Malware Security and Brute-Force Firewall
- Guard Dog Security - WP Fix It
- Hello Dolly
- MainWP Child
- WP Crontrol
- WP phpMyAdmin

✗ Inactive Plugins

- Akismet Anti-spam: Spam Protection
- bbPress
- Better Search Replace
- Classic Widgets
- Core File Monitor
- Fresh Plugins - WP Fix It
- Generate Child Theme
- Gutenberg
- Health Check & Troubleshooting
- Jetpack
- Plugin Check (PCP)
- Rollback Auto Update
- SSL Checker Enhanced
- WooCommerce
- WooCommerce Order Test - WP Fix It
- WP Reset
- WP Rocket

✓ Outdated Plugins

- All plugins are up to date

✓ Abandoned Plugins

- No abandoned plugins found

Installed Themes

Inactive and outdated themes can compromise your website security and functionality. This makes your website much more susceptible to malicious exploits and compatibility issues.

✓ Active Theme

- Twenty Twenty-Three

✗ Inactive Themes

- Astra
- Test Child
- Twenty Twenty-Four
- Twenty Twenty-Two

✓ Outdated Themes

- All themes are up to date

Admin Users

Managing administrative users is vital for WordPress security, as excess or unauthorized admin accounts can increase the risk of unauthorized access and potential breaches.

Username: **jgucci**
Name: **WP Fix It**
Email: **support@wpfixit.com**

SSL Certificate Information

A valid SSL certificate encrypts data, protecting user information and boosting trust. It also improves search engine rankings and ensures your website is marked as secure by browsers.

✓ **Your website has a valid SSL certificate**

HTTPS Enabled: Yes

Certificate Issuer: Let's Encrypt

Certificate Type: Extended Validation (EV)

Issue Date: 08-25-2024

Expiration Date: 11-23-2024

Compliance Check: Meets GDPR and PCI-DSS Requirements

Server PHP Version

Running a supported version of PHP on your website server is essential for security, performance, and compatibility with WordPress and its plugins and themes.

✓ **PHP is running the recommended version 8.2.20**

Recommended PHP Version: 8.0 or higher
WordPress recommends this for optimal performance and security

Minimum Supported PHP Version: 7.4
Older versions are no longer supported and can expose your site to vulnerabilities