Site Audit Report

www.samplesite.com

Table Of Contents

Site Audit Report Checklist

General

PASS	Site free of malware
PASS	Site not listed on blacklists
PASS	Google Transparency Report clear
PASS	Database free of malware and spam
PASS	No suspicious logins
PASS	No successful malware accesses
FAIL	Adequate log files available
PASS	No publicly available logs
PASS	No public phpinfo files
PASS	Site content not at risk for blacklist
PASS	No advertising networks

WordPress Core

PASS	WordPress updated
PASS	WordPress auto-updates are allowed
PASS	wp-config.php secured
PASS	wp-admin file editing disallowed

Themes and Plugins

PASS	Only utilized themes installed
PASS	All themes updated & actively maintained
PASS	Theme core files unmodified
PASS	No high risk theme functions installed
PASS	Only utilized plugins installed
FAIL	All plugins updated & actively maintained
PASS	No high risk plugins installed
PASS	No redundant plugins

Administrative Accounts

PASS	Valid administrative users
PASS	Administrative user emails
PASS	Password audit
PASS	Multisite network administration
PASS	Unique ID for administrators
FAIL	No public transaction or error logs

Wordfence

PASS	Wordfence installed and configured correctly
PASS	Wordfence firewall configured correctly
PASS	Wordfence scanning all files
PASS	Wordfence admin email address entered

Hosting Issues

PASS	Backups being stored
PASS	Site is hosted in its own space
PASS	Linux Hosting
PASS	No web server security issues
PASS	Web server version updated
PASS	No publicly accessible backups
PASS	Backups are frequent
FAIL	SSL installed and configured correctly
PASS	No credit card data stored on site
PASS	File permissions set correctly
PASS	PHP version updated
PASS	No suspicious cron jobs
PASS	End-to-end encryption/No cloud-based WAF
PASS	Strong CPANEL/Hosting Password
PASS	Strong FTP Password
PASS	Using SFTP
PASS	SSH unused or secured
PASS	No .my.cnf files

Database

PASS	Only one MySQL database user
PASS	MySQL user has appropriate permissions
PASS	Strong MySQL database user password
PASS	Remote database access disabled
PASS	No custom MySQL database connections
PASS	PhpMyAdmin updated
FAIL	Tables are optimized
PASS	Database updated

Failure Action Items

General

- ❑ **Adequate log files available.** We did not find adequate log files as your server is only storing 2 weeks of log files, which is not adequate for monitoring intrusions. We recommend that you store 12 months of log files in the event that your site is compromised.

Themes and Plugins

- ❑ **Plugins not updated or actively maintained.** We found plugins that require updates and some plugins that are not actively maintained They include:
  - ❑ **Slider Revolution.** Your site is using version 4.6. The current version is 5.4.1.
  - ❑ **WP Bakery Visual Composer.** Your site is using version 4.12.1. The current version is 5.1.1.
  - ❑ **WP-PagesNav.** Plugin has not been updated in 10 years. We recommend finding an actively maintained alternative.

Administrative Accounts

- ❑ **Public transaction or error logs.** We found public transaction/error logs in wp-content/debug.log. We recommend using htaccess to protect this file.

Hosting Issues

- ❑ **SSL installed and configured correctly.** Your site is not using SSL. We recommend that all sites use SSL for HTTPS encryption.

Database

- ❑ **Custom MySQL database connections.** We found custom MySQL database connections in your site's code. Your site's newsletter template has it's own connections to your database. We recommend recoding this functionality to utilize the wpdb class within WordPress for security reasons.
- ❑ **Tables are not optimized.** Your database tables require optimization for better performance and stability.

Security Elements Reviewed & Remediated

General

- **Site free of malware.** Wordfence scans the site to look for malware, backdoors, trojans, or other malicious scripts.
- **Site not listed on blacklists.** We review the following blacklists to ensure your site is not listed:
    - McAfee Site Advisor
    - Norton SafeWeb
    - etc.
- **Google transparency report clear.** Google's safe browsing transparency report can often indicate problems.
- **Database free of malware.** We reviewed your database to look for spam or malware.
- **No suspicious logins.** We look for logins that appear to be from suspicious locations.
- **No successful malware accesses.** We look for any successful access to malware in the available log files.
- **Adequate log files available.** We look for at least 30 days of log files. We would recommend that you store up to 12 months of log files if possible.
- **No publicly available log files.** We look for any log files, debugging logs, or error logs that are publicly available.
- **No publicly available phpinfo files.** We look for any files that have a phpinfo function that are publicly available. These files can often provide attackers too much information about server configurations.
- **Site content not at risk for blacklist.** Some site content such as pharmaceutical, fashion, or other highly competitive niches, can be at risk for erroneous blacklisting.
- **No advertising networks.** Some advertising networks do not monitor their ad stock well and can be a source of malware served up to site visitors. While the target site is not affected, an ad network can often be a security risk if not effectively managed.

WordPress Core

- **WordPress updated.** Keeping WordPress updated to the most current version ensures all security fixes are installed.
- **WordPress auto-updates are allowed.** We recommend allowing security patches to be automatically applied.
- **wp-config.php is secured.** We look for hash salts within wp-config.php and ensure the file is set with adequate permissions. This file contains database credentials and requires additional security measures.
- **wp-admin file editing disallowed.** If your site is not actively in development, disallowing file editing in wp-config.php limits the damage that can be done if an administrative login is compromised.

Themes and Plugins

- **Only utilized themes installed.** We recommend that you do not have extraneous themes installed.
- **All themes updated and actively maintained.** We check to ensure that the theme(s) installed are updated and are actively maintained by their developers.
- **Theme core files unmodified.** Modifying theme files is not recommended. If you need to make changes, use a child theme.

- **No high risk theme functions installed.** We look for high risk theme functionality such as uploading scripts, remote tunnel access, etc.
- **Only utilized plugins installed.** We recommend that you do not have extraneous plugins installed.
- **All plugins updated and actively maintained.** We check to ensure that all plugins, both premium and repository, are updated to the current versions. We check to see if plugin development appears to be abandoned. We check to ensure installed plugins have been updated in the last 2 years.
- **No high risk plugins installed.** We look for functions within plugins that might allow for uploading, administrative tunnels, etc.
- **No redundant plugins.** We look for plugins that may have overlapping functionality.

Administrative Accounts

- **Valid administrative users.** We check to see that administrative users appear to be valid.
- **Administrative user emails.** We ensure administrative users have email addresses.
- **No Extraneous admin users.** We check to see if there are an inordinate number of administrative users. We recommend limiting administrative access and using contributor, editor, store manager, and other user types.
- **Password audit.** We check to see that all passwords appear to be strong and unique.
- **Multisite network administration.** If your site is a multisite installation, we ensure that you have network administrative capabilities.
- **Unique ID for administrators.** We evaluate whether administrators appear to have unique user IDs and that logins are not shared. Each user should have their own login for PCI compliance.
- **No public transaction or error logs.** We check for any public transaction or error logs that might provide attackers information about your site configuration.

Wordfence

- **Wordfence installed and configured correctly.** We ensure that Wordfence is installed, configured correctly, and that your premium key is installed.
- **Wordfence firewall configured correctly.** We make sure that the Wordfence firewall is installed and optimized for your server. If recently installed, the firewall may be in learning mode. We recommend familiarizing yourself with learning mode to ensure that all site functionality is whitelisted.
- **Wordfence scanning all files.** We ensure that Wordfence is scanning all installed files, other than some binary files.
- **Wordfence administrative user email entered.** We ensure that an administrative email is configured to receive reports about site issues requiring attention.

Hosting Issues

- **Backups being stored.** We look for evidence that backups are being made of your site.
- **Linux hosting.** We verify that your site is running on a linux server environment.
- **No web server security issues.** We look for known web server security issues.
- **No publicly accessible backups.** We look for publicly available backups that might contain sensitive site information.
- **Backups are frequent.** We evaluate that your site is being backed up adequately.
- **SSL installed and configured correctly.** We look to see that the site has an SSL certificate installed and configured correctly. SSL certificates ensure that site traffic between your server and your site visitors is encrypted.

- **No credit card data stored on site.** We look for evidence of credit card information stored on your site or in your database.
- **File permissions set correctly.** We check to see that file and directory permissions appear to be set correctly.
- **PHP version updated.** We look to see that the server is running an updated version of PHP.
- **No suspicious cron jobs.** We look for suspicious cron jobs.
- **End-to-end encryption/cloud-based WAF.** We look for evidence of cloud-based WAF breaking encryption.
- **Strong cpanel/hosting password.** We evaluate whether the hosting panel password is strong and appears to be unique from other passwords.
- **Strong FTP password.** We check to see if the FTP password is strong and appears to be unique from other passwords.
- **Using SFTP.** We check to see if the site is using SFTP to ensure for secure file transfers.
- **SSH unused or secured.** We check to see if the site has SSH secured or disabled.
- **No .my.cnf files.** We check for any .my.cnf files in your hosting account containing sensitive credentials.

Database

- **Only one MySQL database user.** We look for extra MySQL database users.
- **MySQL user has appropriate permissions.** We ensure the MySQL database user has appropriate permissions to access and modify the database.
- **Strong MySQL database user password.** We evaluate the MySQL database user's password.
- **Remote database access disabled.** We look for remote database access capabilities on your site.
- **No custom MySQL database connections.** We review the site code to look for any extraneous database connections.
- **PhpMyAdmin updated.** We determine if the host's version of PhpMyAdmin does not have security issues.
- **Tables are optimized.** We check to see if database tables require optimization.
- **Database version updated.** We ensure that the database version is adequately updated.