EXECUTIVE REPORT

WEBSITE AUDIT REPORT

MADE FOR:
https://wpaudit-sandbox.sandywp.dev

REPORT INFO:
Audited on: September 1, 2026
Tracking ID: #UWPA-378617



71%
OVERALL SCORE

209
PASSED AUDITS

33
WARNINGS

13
CRITICAL RISKS

Comprehensive Security, Performance, SEO & Infrastructure Audit

Generated by SS Internet Services (https://ssinternet.in) • 100% Privacy & Transparent AI Data Processing

Understanding Your Website Audit Report

Thank you for choosing us to audit your digital presence. This comprehensive report analyzes your website's performance, security, SEO, and infrastructure to ensure you are operating at peak efficiency.

Why This Audit Matters

Your website health directly impacts user experience, search engine rankings, and ultimately, your revenue. The insights in this report provide a clear, prioritized roadmap to strengthen your digital foundation and outperform competitors.

How to Read This Report

Each category of your website is scored from 0 to 100 based on industry best practices:

- **Good (80-100): Optimal and safe. Minimal action required.**
- **Fair (50-79): Requires review and optimization to prevent issues.**
- **Critical (0-49): Urgent remediation needed to avoid severe impact.**

Next Steps

Review the Executive Summary and Category findings in the following pages. We are ready to help you implement these recommended fixes and maximize your digital ROI. Please reach out to discuss your personalized action plan.

© 2026 SS Internet Services
https://ssinternet.in
© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

TABLE OF CONTENTS

REPORT NAVIGATION INDEX

01	Executive Summary & Dashboard	P. 4	
02	Security Audit & Findings	P. 6	
03	Performance Audit & Findings	P. 12	
04	Seo Audit & Findings	P. 15	
05	Safety Audit & Findings	P. 19	
06	Accessibility Audit & Findings	P. 22	
07	Database Audit & Findings	P. 23	
08	Ssl Audit & Findings	P. 25	
09	Compliance Audit & Findings	P. 26	
10	Content Audit & Findings	P. 28	
11	Core Web Vitals Audit & Findings	P. 30	
12	Ecommerce Audit & Findings	P. 32	
13	Environment Audit & Findings	P. 34	
14	Advanced Schema Audit & Findings	P. 36	
15	Api Security Audit & Findings	P. 37	
16	Internationalization Audit & Findings	P. 38	
17	Multisite Audit & Findings	N/A P. 39	
18	Backup Recovery Audit & Findings	P. 40	
19	Advanced Security Audit & Findings	P. 41	

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

EXECUTIVE SUMMARY

OVERVIEW & KEY METRICS

71%	209	33	13
OVERALL SCORE	PASSED CHECKS	WARNINGS	CRITICAL RISKS

AI INTELLIGENCE EXECUTIVE SUMMARY

Your site analysis is complete. Critical security or operational risks have been detected in Security, Safety, Compliance, Content, requiring immediate remediation. Core categories like Accessibility, Environment remain healthy and stable.

AUDIT CATEGORY	HEALTH SCORE	STATUS GRADE	ACTION REQUIRED
Security	71%	FAIR	Review Warnings
Performance	85%	GOOD	Optimal / Safe
Seo	90%	GOOD	Optimal / Safe
Safety	79%	FAIR	Review Warnings
Accessibility	100%	GOOD	Optimal / Safe
Database	97%	GOOD	Optimal / Safe
Ssl	90%	GOOD	Optimal / Safe
Compliance	25%	CRITICAL	Immediate Fix Required
Content	25%	CRITICAL	Immediate Fix Required
Core_web_vitals	90%	GOOD	Optimal / Safe
Ecommerce	60%	FAIR	Review Warnings
Environment	100%	GOOD	Optimal / Safe
Advanced_schema	40%	CRITICAL	Immediate Fix Required

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

Api_security	**53%**	**FAIR**	Review Warnings
Internationalization	**38%**	**CRITICAL**	Immediate Fix Required
Multisite	**-1%**	**N/A**	Not Applicable / Optional
Backup_recovery	**70%**	**FAIR**	Review Warnings
Advanced_security	**100%**	**GOOD**	Optimal / Safe

© 2026 SS Internet Services
https://ssinternet.in
© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

Security Health Overview

71%

AI INTELLIGENCE CATEGORY INSIGHTS

The audit reveals critical security risks including debug mode enabled, file editing enabled, default wp_ database prefix, XML-RPC enabled, and wp-config.php writable, posing severe attack surface exposure. Despite passing SSL/HTTPS and PHP version checks, these findings highlight immediate remediation needs to harden the WordPress environment against exploitation.

STATUS	AUDIT CHECK	FINDINGS & STEP-BY-STEP FIX PLAN
PASSED	WordPress Updates	WordPress 7.1 is current.
PASSED	SSL/HTTPS	Site uses HTTPS.
WARNING	Debug Mode	Debug mode enabled. [Risk Impact: 55/100] AI Reasoning: • Disable on production. • Diagnostic details: Debug mode enabled. Remediation Action Plan: • Disable on production. • Diagnostic details: Debug mode enabled.
WARNING	File Editing	File editing enabled. [Risk Impact: 80/100] AI Reasoning: • Step 1: Add the following line to wp-config.php to disable file editing: `define('DISALLOW_FILE_EDIT', true);` • Step 2: Verify by attempting to access the file editor from the WordPress dashboard; it should be blocked Remediation Action Plan: • Step 1: Add the following line to wp-config.php to disable file editing: `define('DISALLOW_FILE_EDIT', true);` • Step 2: Verify by attempting to access the file editor from the WordPress dashboard; it should be blocked
PASSED	PHP Version	PHP 8.3.33
WARNING	Admin Username	"admin" user exists. [Risk Impact: 55/100] AI Reasoning: • Rename the admin user. • Diagnostic details: "admin" user exists. Remediation Action Plan:

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

		• Rename the admin user. • Diagnostic details: "admin" user exists.
PASSED	Plugin Updates	All plugins are current.
PASSED	Theme Updates	All themes are current.
WARNING	Database Prefix	Using default "wp_" prefix. [Risk Impact: 55/100] AI Reasoning: • Use a custom database prefix. • Diagnostic details: Using default "wp_" prefix. Remediation Action Plan: • Use a custom database prefix. • Diagnostic details: Using default "wp_" prefix.
WARNING	XML-RPC	XML-RPC is enabled. [Risk Impact: 70/100] AI Reasoning: • Step 1: Add the following line to wp-config.php to disable XML-RPC: `define('XMLRPC_ENABLED', false);` • Step 2: Confirm XML-RPC is disabled by checking the WordPress dashboard; it should no longer be available Remediation Action Plan: • Step 1: Add the following line to wp-config.php to disable XML-RPC: `define('XMLRPC_ENABLED', false);` • Step 2: Confirm XML-RPC is disabled by checking the WordPress dashboard; it should no longer be available
PASSED	REST API Users	REST API users endpoint protected.
INFO	Directory Listing	Upload directory not configured.
CRITICAL	wp-config Permissions	wp-config.php is writable! [Risk Impact: 95/100] AI Reasoning: • Step 1: Secure wp-config.php by setting correct file permissions: `chmod 600 /path/to/your/site/wp-config.php` • Step 2: Ensure file ownership is restricted to the web server user: `chown www-data:www-data /path/to/your/site/wp-config.php` Remediation Action Plan: • Step 1: Secure wp-config.php by setting correct file permissions: `chmod 600 /path/to/your/site/wp-config.php` • Step 2: Ensure file ownership is restricted to the web server user: `chown www-data:www-data /path/to/your/site/wp-config.php`
WARNING	Security Headers	Missing: x-content-type-options, x-frame-options, x-xss-protection [Risk Impact: 55/100]

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

		AI Reasoning: • Add security headers. • Diagnostic details: Missing: x-content-type-options, x-frame-options, x-xss-protection Remediation Action Plan: • Add security headers. • Diagnostic details: Missing: x-content-type-options, x-frame-options, x-xss-protection
WARNING	Core File Permissions	wp-includes is writable. [Risk Impact: 55/100] AI Reasoning: • Set to 755. • Diagnostic details: wp-includes is writable. Remediation Action Plan: • Set to 755. • Diagnostic details: wp-includes is writable.
CRITICAL	Sensitive Files	Exposed: readme.html, license.txt [Risk Impact: 88/100] AI Reasoning: • Remove or protect these files. • Diagnostic details: Exposed: readme.html, license.txt Remediation Action Plan: • Remove or protect these files. • Diagnostic details: Exposed: readme.html, license.txt
PASSED	Two-Factor Auth	2FA plugin detected.
PASSED	Login Security	Login protection active.
WARNING	Content Security Policy	No CSP header found. [Risk Impact: 55/100] AI Reasoning: • Add CSP to prevent XSS attacks. • Diagnostic details: No CSP header found. Remediation Action Plan: • Add CSP to prevent XSS attacks. • Diagnostic details: No CSP header found.
PASSED	Cookie Security	Cookies have proper security attributes.
CRITICAL	Upload PHP Execution	PHP may execute in uploads folder. [Risk Impact: 88/100] AI Reasoning: • Add .htaccess with php_flag engine off. • Diagnostic details: PHP may execute in uploads folder.

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

		Remediation Action Plan: • Add .htaccess with php_flag engine off. • Diagnostic details: PHP may execute in uploads folder.
PASSED	Suspicious Files	No suspicious files detected.
PASSED	Hidden Files	No suspicious hidden files.
PASSED	Theme Integrity	Theme is up to date.
PASSED	Exposed DB Credentials	wp-config.php protected.
PASSED	PHP Test Files	No test files exposed.
PASSED	Backup Files	No backup files exposed.
PASSED	SQL Injection Defense	No SQL errors detected.
PASSED	Core Integrity	Core files match official signatures.
PASSED	Plugin File Integrity	Sampled plugin files match official WordPress.org releases (5 checked).
PASSED	User Enumeration	Author enumeration blocked.
WARNING	HSTS Header	No HSTS header. [Risk Impact: 55/100] AI Reasoning: • Add Strict-Transport-Security header. • Diagnostic details: No HSTS header. Remediation Action Plan: • Add Strict-Transport-Security header. • Diagnostic details: No HSTS header.
WARNING	X-Frame-Options	Missing X-Frame-Options. [Risk Impact: 55/100] AI Reasoning: • Add header to prevent clickjacking. • Diagnostic details: Missing X-Frame-Options. Remediation Action Plan: • Add header to prevent clickjacking. • Diagnostic details: Missing X-Frame-Options.
WARNING	MIME Sniffing	Missing nosniff header.

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

		[Risk Impact: 55/100] AI Reasoning: • Add X-Content-Type-Options: nosniff. • Diagnostic details: Missing nosniff header. Remediation Action Plan: • Add X-Content-Type-Options: nosniff. • Diagnostic details: Missing nosniff header.
INFO	**Referrer Policy**	No Referrer Policy. Recommendation: Control info leakage with Referrer-Policy.
PASSED	**SQL Injection Scan**	No SQL/code injection patterns detected.
INFO	**Application Passwords**	Application passwords enabled. Recommendation: Disable if not needed.
PASSED	**Cloudflare Detection**	Cloudflare detected via DNS.
WARNING	**WAF Detection**	No WAF detected. [Risk Impact: 55/100] AI Reasoning: • Install a Web Application Firewall. • Diagnostic details: No WAF detected. Remediation Action Plan: • Install a Web Application Firewall. • Diagnostic details: No WAF detected.
WARNING	**Rate Limiting**	No rate limiting detected. [Risk Impact: 55/100] AI Reasoning: • Implement rate limiting to prevent abuse. • Diagnostic details: No rate limiting detected. Remediation Action Plan: • Implement rate limiting to prevent abuse. • Diagnostic details: No rate limiting detected.
PASSED	**IP Blocking**	IP blocking configured: wordfence
PASSED	**Bot Detection**	Bot detection active: wordfence
WARNING	**Readme Security**	readme.html is publicly accessible. [Risk Impact: 55/100] AI Reasoning: • Remove or block readme.html file.

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

		• Diagnostic details: readme.html is publicly accessible. Remediation Action Plan: • Remove or block readme.html file. • Diagnostic details: readme.html is publicly accessible.
CRITICAL	Install.php Security	install.php is accessible! [Risk Impact: 88/100] AI Reasoning: • Block or remove install.php. • Diagnostic details: install.php is accessible! Remediation Action Plan: • Block or remove install.php. • Diagnostic details: install.php is accessible!
CRITICAL	Debug Log Security	debug.log is publicly accessible! [Risk Impact: 88/100] AI Reasoning: • Block or remove debug.log file. • Diagnostic details: debug.log is publicly accessible! Remediation Action Plan: • Block or remove debug.log file. • Diagnostic details: debug.log is publicly accessible!
WARNING	PHPMailer	PHPMailer not detected. [Risk Impact: 55/100] AI Reasoning: • Ensure WordPress is intact. • Diagnostic details: PHPMailer not detected. Remediation Action Plan: • Ensure WordPress is intact. • Diagnostic details: PHPMailer not detected.
INFO	jQuery Version	jQuery version not detected.

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

Performance Health Overview

85%

AI INTELLIGENCE CATEGORY INSIGHTS

The audit reveals missing compression and absent caching headers, exposing the site to increased latency, bandwidth waste, and cachepoisoning vectors, while the high script count (19) and unoptimized asset delivery broaden the XSS and resourceexhaustion attack surface. Passes on page load time, active plugin count, and memory limit demonstrate a solid performance baseline and ample PHP memory allocation.

STATUS	AUDIT CHECK	FINDINGS & STEP-BY-STEP FIX PLAN
PASSED	Page Load Time	0.3s - excellent!
PASSED	Active Plugins	5 active plugins.
PASSED	Memory Limit	Memory: 256M
INFO	Object Cache	No external object cache. Recommendation: Consider Redis or Memcached.
PASSED	Max Execution Time	300s (0=unlimited)
WARNING	Compression	No compression detected. [Risk Impact: 85/100] AI Reasoning: • Step 1: Enable gzip/deflate compression at the web server level. • Step 2: For Apache add "<IfModule mod_deflate.c>\n AddOutputFilterByType DEFLATE text/html text/css application/javascript\n</IfModule>" to .htaccess or for Nginx add "gzip on; gzip_types text/css application/javascript;" in the server block. Remediation Action Plan: • Step 1: Enable gzip/deflate compression at the web server level. • Step 2: For Apache add "<IfModule mod_deflate.c>\n AddOutputFilterByType DEFLATE text/html text/css application/javascript\n</IfModule>" to .htaccess or for Nginx add "gzip on; gzip_types text/css application/javascript;" in the server block.
WARNING	Browser Caching	No caching headers. [Risk Impact: 85/100] AI Reasoning: • Step 1: Set longterm caching headers for static assets. • Step 2: In .htaccess add "<IfModule mod_expires.c>\n ExpiresActive On\n ExpiresByType text/css "access 1 year"\n ExpiresByType application/javascript "access 1 year"\n</IfModule>" or in Nginx add "location ~* \.(css|js)$ { expires 1y; add_header Cache-Control \"public, immutable\"; }".

© 2026 SS Internet Services
https://ssinternet.in
© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

		Remediation Action Plan: • Step 1: Set longterm caching headers for static assets. • Step 2: In .htaccess add "<IfModule mod_expires.c>\n ExpiresActive On\n ExpiresByType text/css "access 1 year"\n ExpiresByType application/javascript "access 1 year"\n</IfModule>" or in Nginx add "location ~* \.(css|js)$ { expires 1y; add_header Cache-Control \"public, immutable\"; }".
PASSED	Vary Header	Vary header present.
PASSED	Upload Max Size	Max upload: 256M
PASSED	WP Cron	24 scheduled tasks.
PASSED	Autoloaded Data	0 MB autoloaded.
PASSED	Page Size	82 KB homepage.
WARNING	Asset Count	19 scripts, ~35 styles. [Risk Impact: 85/100] AI Reasoning: • Step 1: Consolidate and minify CSS/JS to reduce HTTP requests. • Step 2: Use WPCLI to generate a combined asset bundle: "wp asset-cleanup combine --type=js --output=wp-content/uploads/combined.min.js && wp asset-cleanup combine --type=css --output=wp-content/uploads/combined.min.css" and enqueue the bundled files in functions.php. Remediation Action Plan: • Step 1: Consolidate and minify CSS/JS to reduce HTTP requests. • Step 2: Use WPCLI to generate a combined asset bundle: "wp asset-cleanup combine --type=js --output=wp-content/uploads/combined.min.js && wp asset-cleanup combine --type=css --output=wp-content/uploads/combined.min.css" and enqueue the bundled files in functions.php.
INFO	CDN Detection	No CDN detected. Recommendation: Consider using a CDN.
PASSED	Critical CSS	Critical CSS optimization detected.
PASSED	Font Optimization	No external fonts detected.
WARNING	Server Caching Headers	No caching headers. [Risk Impact: 85/100] AI Reasoning: • Step 1: Instruct the server to emit CacheControl for dynamic pages where appropriate. • Step 2: Add to .htaccess "<IfModule mod_headers.c>\n Header set Cache-Control \"private, max-age=0, must-revalidate\"\n</IfModule>" or in Nginx "add_header Cache-Control \"private, max-age=0, must-revalidate\";" inside the

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

		location block for PHP. Remediation Action Plan: • Step 1: Instruct the server to emit CacheControl for dynamic pages where appropriate. • Step 2: Add to .htaccess "<IfModule mod_headers.c>\n Header set Cache-Control \"private, max-age=0, must-revalidate\"\n</IfModule>" or in Nginx "add_header Cache-Control \"private, max-age=0, must-revalidate\";" inside the location block for PHP.
INFO	**DNS Prefetch**	DNS prefetch not detected. Recommendation: Add DNS prefetch for external domains.
INFO	**Resource Hints**	No resource hints found. Recommendation: Add preconnect for critical origins.
WARNING	**Script Files**	19 script tags. [Risk Impact: 85/100] AI Reasoning: • Step 1: Defer or async noncritical scripts to improve render blocking. • Step 2: In functions.php replace each wp_enqueue_script call with "wp_enqueue_script($handle, $src, $deps, $ver, true);" and add "wp_script_add_data($handle, 'async', true);" or "wp_script_add_data($handle, 'defer', true);" for applicable handles. Remediation Action Plan: • Step 1: Defer or async noncritical scripts to improve render blocking. • Step 2: In functions.php replace each wp_enqueue_script call with "wp_enqueue_script($handle, $src, $deps, $ver, true);" and add "wp_script_add_data($handle, 'async', true);" or "wp_script_add_data($handle, 'defer', true);" for applicable handles.
PASSED	**CSS Files**	5 stylesheets.
INFO	**Keep-Alive**	Keep-alive not detected.

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

Seo Health Overview

90%

AI INTELLIGENCE CATEGORY INSIGHTS

The audit surfaces SEOrelated attack vectors: a default tagline and missing Open Graph tags can be leveraged for brand impersonation, while a short title and absent meta description degrade clickthrough security signals; a broken internal link creates 404 endpoints that attackers may exploit for phishing redirects. All other core SEO configurations are sound, confirming a hardened permalink structure and controlled search visibility.

STATUS	AUDIT CHECK	FINDINGS & STEP-BY-STEP FIX PLAN
PASSED	Search Visibility	Search engines allowed.
WARNING	Tagline	Default or empty tagline. [Risk Impact: 85/100] AI Reasoning: • Step 1: Update the site tagline to a unique, brandspecific string. • Step 2: wp option update blogdescription "Your Unique Tagline Here" Remediation Action Plan: • Step 1: Update the site tagline to a unique, brandspecific string. • Step 2: wp option update blogdescription "Your Unique Tagline Here"
PASSED	Permalinks	SEO-friendly permalinks.
WARNING	Title Tag	Title length: 17 chars [Risk Impact: 85/100] AI Reasoning: • Step 1: Extend the title length to meet SEO best practices (3560 chars). • Step 2: wp post meta update $(wp post list --post_type=page --field=ID) _aioseo_title "Your Expanded Title Including Primary Keyword" Remediation Action Plan: • Step 1: Extend the title length to meet SEO best practices (3560 chars). • Step 2: wp post meta update $(wp post list --post_type=page --field=ID) _aioseo_title "Your Expanded Title Including Primary Keyword"
WARNING	Meta Description	No meta description found. [Risk Impact: 85/100] AI Reasoning: • Step 1: Insert a meta description tag for all singular templates. • Step 2: Add to the active theme's `header.php`: <?php if (is_singular()) { echo '<meta name="description" content="Your concise, keywordrich description here">'; } ?> Remediation Action Plan: • Step 1: Insert a meta description tag for all singular templates. • Step 2: Add to the active theme's `header.php`:

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

		<?php if (is_singular()) { echo '<meta name="description" content="Your concise, keywordrich description here">'; } ?>
PASSED	H1 Tag	Single H1 tag found.
PASSED	XML Sitemap	Sitemap found.
PASSED	Robots.txt	Robots.txt exists.
PASSED	Open Graph	Open Graph tags found.
PASSED	Canonical Tag	Canonical tag found.
PASSED	Schema Markup	Structured data found.
PASSED	Mobile Viewport	Viewport meta found.
PASSED	Mixed Content	No mixed content issues.
PASSED	SEO Plugin	SEO capability detected: Yoast SEO v28.3
PASSED	Hreflang Tags	No hreflang (OK for single-language sites).
PASSED	404 Page	Correct 404 status code returned.
PASSED	URL Structure	Clean URL structure.
PASSED	Core Web Vitals	Good performance info for SEO.
WARNING	Internal Links	1 broken internal links found. [Risk Impact: 85/100] AI Reasoning: • Step 1: Locate and replace the broken URL. • Step 2: wp search-replace 'https://wpaudit-sandbox.sandywp.dev/old-broken-link' 'https://wpaudit-sandbox.sandywp.dev/new-target' --dry-run && wp search-replace 'https://wpaudit-sandbox.sandywp.dev/old-broken-link' 'https://wpaudit-sandbox.sandywp.dev/new-target' --yes Remediation Action Plan: • Step 1: Locate and replace the broken URL. • Step 2: wp search-replace 'https://wpaudit-sandbox.sandywp.dev/old-broken-link' 'https://wpaudit-sandbox.sandywp.dev/new-target' --dry-run && wp search-replace 'https://wpaudit-sandbox.sandywp.dev/old-broken-link' 'https://wpaudit-sandbox.sandywp.dev/new-target' --yes

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

PASSED	External Links	No broken external links (checked 1).
PASSED	Broken Images	No broken images detected.
PASSED	Redirect Chains	No redirect chains detected.
INFO	Twitter Cards	Limited Twitter Card implementation. Recommendation: Add Twitter Card meta tags.
WARNING	Open Graph	Incomplete Open Graph: 3/5 tags. [Risk Impact: 85/100] AI Reasoning: • Step 1: Add the missing Open Graph meta tags to the head. • Step 2: Insert into `functions.php`: add_action('wp_head', function(){ if (is_singular()) { echo '<meta property="og:title" content="'.get_the_title().'">'; echo '<meta property="og:description" content="'.wp_strip_all_tags(get_the_excerpt()).'">'; echo '<meta property="og:url" content="'.get_permalink().'">'; echo '<meta property="og:type" content="article">'; echo '<meta property="og:image" content="'.get_the_post_thumbnail_url(null, 'full').'">'; } }); Remediation Action Plan: • Step 1: Add the missing Open Graph meta tags to the head. • Step 2: Insert into `functions.php`: add_action('wp_head', function(){ if (is_singular()) { echo '<meta property="og:title" content="'.get_the_title().'">'; echo '<meta property="og:description" content="'.wp_strip_all_tags(get_the_excerpt()).'">'; echo '<meta property="og:url" content="'.get_permalink().'">'; echo '<meta property="og:type" content="article">'; echo '<meta property="og:image" content="'.get_the_post_thumbnail_url(null, 'full').'">'; } });
INFO	Pinterest Rich Pins	No Pinterest Rich Pins detected. Recommendation: Add Pinterest meta tags if targeting Pinterest users.
INFO	LinkedIn Tags	No LinkedIn article tags. Recommendation: LinkedIn uses Open Graph - ensure OG tags are present.
PASSED	Social Sharing	Social sharing elements detected.
INFO	Navigation Menu	No primary menu found. Recommendation: Create navigation menus to avoid orphaned pages.

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

INFO	Title Length	17 characters. Recommendation: Optimal title length is 50-60 characters.
PASSED	Clean URLs	Clean permalink structure.

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

Safety Health Overview

79%

AI INTELLIGENCE CATEGORY INSIGHTS

The audit reveals critical security gaps including suspicious code in a plugin, missing SPF/DNS records, and a blacklisted IP, alongside a warning about debug logging. These expose the site to injection attacks, email spoofing, and potential blacklist escalation, while also presenting a performance bottleneck from debug logging overhead.

STATUS	AUDIT CHECK	FINDINGS & STEP-BY-STEP FIX PLAN
PASSED	Theme Inventory	3 theme(s) installed (1 active, 2 inactive). All up to date. Active Theme: Twenty Twenty-Five v1.5 by the WordPress team. Recommendation: Active Theme: Twenty Twenty-Five v1.5 | Author: the WordPress team | Website: https://wordpress.org/themes/twentytwentyfive/ • Installed Themes (3): • Twenty Twenty-Five v1.5 by the WordPress team [ACTIVE] • Twenty Twenty-Four v1.6 by the WordPress team [Inactive] • Twenty Twenty-Three v1.7 by the WordPress team [Inactive]
PASSED	Plugin Inventory	5 plugins installed. All up to date. Recommendation: All-in-One WP Migration and Backup v7.110, Ultimate WP Audit Agent v2.0.0, WooCommerce v11.0.1, Wordfence Security v9.0.0, Yoast SEO v28.3
PASSED	Backup Plugin	Backup capability detected: All-in-One WP Migration and Backup v7.110
PASSED	Security Plugin	Security capability detected: Wordfence Security v9.0.0
PASSED	Admin Email	Valid admin email configured.
PASSED	Inactive Themes	2 inactive themes.
PASSED	Inactive Plugins	0 inactive plugins.
INFO	File Modifications	File modifications allowed. Recommendation: Consider DISALLOW_FILE_MODS.
INFO	Auto Updates	Auto-updates not fully enabled. Recommendation: Enable auto-updates.
WARNING	Debug Logging	Debug logging enabled. [Risk Impact: 70/100]

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

		AI Reasoning: • 1. Disable debug logging by setting `WP_DEBUG` to `false` in `wp-config.php`. • 2. Flush WordPress rewrite rules with `wp rewrite flush` to ensure changes take effect. Remediation Action Plan: • 1. Disable debug logging by setting `WP_DEBUG` to `false` in `wp-config.php`. • 2. Flush WordPress rewrite rules with `wp rewrite flush` to ensure changes take effect.
PASSED	Script Debug	SCRIPT_DEBUG disabled.
PASSED	Script Concatenation	Script concatenation enabled.
CRITICAL	Core Code Integrity	Suspicious code in: wp-content/plugins/ultimate-audit-agent/ultimate-audit-agent.php [Risk Impact: 95/100] AI Reasoning: • 1. Identify and isolate the plugin `ultimate-audit-agent` causing the critical code integrity warning. • 2. Remove or replace the plugin with a trusted alternative, ensuring no malicious code remains. • 3. Run `wp plugin list --status=inactive` to verify no remnants of the plugin persist. Remediation Action Plan: • 1. Identify and isolate the plugin `ultimate-audit-agent` causing the critical code integrity warning. • 2. Remove or replace the plugin with a trusted alternative, ensuring no malicious code remains. • 3. Run `wp plugin list --status=inactive` to verify no remnants of the plugin persist.
CRITICAL	Email Security	SPF and DMARC missing. [Risk Impact: 88/100] AI Reasoning: • Configure email authentication. • Diagnostic details: SPF and DMARC missing. Remediation Action Plan: • Configure email authentication. • Diagnostic details: SPF and DMARC missing.
CRITICAL	Blacklist Status	IP 172.67.188.37 is blacklisted. [Risk Impact: 88/100] AI Reasoning: • Contact hosting provider. • Diagnostic details: IP 172.67.188.37 is blacklisted. Remediation Action Plan: • Contact hosting provider. • Diagnostic details: IP 172.67.188.37 is blacklisted.
PASSED	Abandoned Plugins	All plugins actively maintained.

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

PASSED	Plugin Conflicts	No plugin conflicts detected.
PASSED	Duplicate Functionality	No duplicate functionality.
INFO	Plugin Load	Resource-heavy: WooCommerce Recommendation: Monitor performance.
INFO	External API Calls	Plugins with API calls: ultimate-audit-agent Recommendation: Ensure trusted.
PASSED	Uploads PHP Files	No PHP files found in uploads directory.

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

Accessibility Health Overview

100%

AI INTELLIGENCE CATEGORY INSIGHTS

The audit confirms that core accessibility controls—HTML language attribute, viewport meta tag, and hierarchical heading markup—are correctly implemented, eliminating common injection vectors such as DOMbased XSS via malformed language tags and viewportrelated layout attacks. With a clean surface, the next enterprise hardening milestone is to enforce a strict ContentSecurityPolicy with noncebased script allowances and enable HTTP/3 with QUIC for optimal performance.

STATUS	AUDIT CHECK	FINDINGS & STEP-BY-STEP FIX PLAN
PASSED	HTML Lang	Language attribute set.
PASSED	Viewport Meta	Viewport meta tag present.
PASSED	Heading Structure	Heading structure is valid.
PASSED	Zoom Prevention	Viewport allows zooming.
PASSED	Form Labels	Form check passed.
PASSED	ARIA Landmarks	Landmarks found (Semantic HTML/Roles).
PASSED	Link Text	Link text appears descriptive.
PASSED	Video Captions	Multimedia elements accessible.
PASSED	ARIA Labels	Interactive elements have labels.
PASSED	Mobile Viewport	Responsive viewport configured.
PASSED	Touch Targets	Touch targets appear adequate.
PASSED	Mobile Font Size	Font sizes appear mobile-friendly.
PASSED	Horizontal Scroll	No obvious horizontal scroll issues.
PASSED	Mobile Page Speed	0.27s - excellent mobile speed!

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

Database Health Overview

97%

AI INTELLIGENCE CATEGORY INSIGHTS

The audit reveals a critical database performance bottleneck with 140 table lock waits, potentially causing query delays and resource contention. While other checks pass, this lock contention should be addressed to maintain site responsiveness under load.

STATUS	AUDIT CHECK	FINDINGS & STEP-BY-STEP FIX PLAN
PASSED	Post Revisions	0 revisions.
PASSED	Spam Comments	0 spam comments.
PASSED	Transients	78 transients.
PASSED	Trashed Posts	0 trashed items.
PASSED	Auto-Drafts	1 auto-drafts.
PASSED	Database Engine	Using InnoDB engine.
PASSED	Max Packet Size	16 MB
PASSED	Orphaned Meta	0 orphaned postmeta.
PASSED	Database Overhead	3 MB overhead.
PASSED	Autoloaded Data	0 MB (Excellent).
PASSED	Slow Queries	No slow queries detected.
PASSED	Missing Indexes	All tables have indexes.
PASSED	N+1 Queries	2 queries for 1 posts.
PASSED	Table Sizes	Total DB size: 6.63MB
INFO	DB Optimization	1 recommendations.

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

		Recommendation: Optimize wp_options
PASSED	InnoDB Buffer	Buffer Pool: 128MB
INFO	Query Cache	Query cache disabled (standard for MySQL 8+ or InnoDB).
WARNING	Table Locks	140 table lock waits. [Risk Impact: 85/100] AI Reasoning: • 1. Identify the specific tables causing lock waits using `SHOW ENGINE INNODB STATUS;` and analyze the `LOCK WAIT` section. • 2. Optimize queries accessing those tables by adding appropriate indexes or refactoring to reduce row-level contention. • 3. Implement query caching with `wp option get rewrite_rules` to ensure fast retrieval of frequently accessed data. • 4. Consider sharding large tables or using read replicas to distribute load and reduce lock contention. Remediation Action Plan: • 1. Identify the specific tables causing lock waits using `SHOW ENGINE INNODB STATUS;` and analyze the `LOCK WAIT` section. • 2. Optimize queries accessing those tables by adding appropriate indexes or refactoring to reduce row-level contention. • 3. Implement query caching with `wp option get rewrite_rules` to ensure fast retrieval of frequently accessed data. • 4. Consider sharding large tables or using read replicas to distribute load and reduce lock contention.
INFO	Binary Logs	Binary logging disabled. Recommendation: Enable for point-in-time recovery.
PASSED	Connections	Max connections: 151

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

Ssl Health Overview

90%

AI INTELLIGENCE CATEGORY INSIGHTS

The site runs an outdated OpenSSL 3.5.6 TLS version, exposing it to known vulnerabilities, while the Let's Encrypt DV certificate is valid for 49 days, nearing expiration. Attack surface is the TLS version and certificate expiration; performance bottleneck is the outdated TLS stack.

STATUS	AUDIT CHECK	FINDINGS & STEP-BY-STEP FIX PLAN
PASSED	SSL Expiration	Certificate valid for 49 days.
PASSED	Certificate Issuer	Let's Encrypt (DV)
WARNING	TLS Version	OpenSSL/3.5.6 - outdated. [Risk Impact: 85/100] AI Reasoning: • Step 1: Upgrade OpenSSL to version 3.5.7 or newer by reinstalling the package or using your package manager (e.g., `sudo apt-get install openssl=3.5.7-1+ubuntu20.04.1+deb.sjl`). • Step 2: Restart the web server (e.g., `sudo systemctl restart nginx` or `sudo systemctl restart apache2`) to apply the new TLS configuration. Remediation Action Plan: • Step 1: Upgrade OpenSSL to version 3.5.7 or newer by reinstalling the package or using your package manager (e.g., `sudo apt-get install openssl=3.5.7-1+ubuntu20.04.1+deb.sjl`). • Step 2: Restart the web server (e.g., `sudo systemctl restart nginx` or `sudo systemctl restart apache2`) to apply the new TLS configuration.
PASSED	Cipher Suite	Modern cipher suites detected.
PASSED	SSL Grade	Estimated grade: A (based on config).

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

Compliance Health Overview

25%

AI INTELLIGENCE CATEGORY INSIGHTS

The audit exposes critical regulatory non-compliance vectors across GDPR, CCPA, and ADA/WCAG accessibility mandates, introducing severe legal exposure and automated compliance scraper profiling. Lack of mandated privacy policies, terms of service, and cookie consent mechanisms leaves user data processing unconsented and vulnerable to statutory financial penalties. Remediation requires programmatic instantiation of legal pages, deployment of explicit consent management architectures, and structural DOM/aria remediation for WCAG compliance.

STATUS	AUDIT CHECK	FINDINGS & STEP-BY-STEP FIX PLAN
WARNING	GDPR Compliance	No GDPR compliance indicators detected. [Risk Impact: 85/100] AI Reasoning: • Deploy a zero-cookie-until-consent mechanism using WP-CLI to install and activate an enterprise Cookie Consent Banner framework with script-blocking capabilities. • wp plugin install cookie-notice --activate && wp option update cookie_notice_options '{"geotargeting":true,"blocking":true}' --format=json Remediation Action Plan: • Deploy a zero-cookie-until-consent mechanism using WP-CLI to install and activate an enterprise Cookie Consent Banner framework with script-blocking capabilities. • wp plugin install cookie-notice --activate && wp option update cookie_notice_options '{"geotargeting":true,"blocking":true}' --format=json
INFO	CCPA Compliance	No CCPA indicators. Required if serving California users.
CRITICAL	WCAG Level	Below WCAG Level A. [Risk Impact: 90/100] AI Reasoning: • Enforce automated accessibility linting in the theme CI/CD pipeline and inject global aria-labels, semantic HTML landmarks, and contrast fixes programmatically. • wp theme mod set accessibility_ready true && wp plugin install WP-Accessibility --activate Remediation Action Plan: • Enforce automated accessibility linting in the theme CI/CD pipeline and inject global aria-labels, semantic HTML landmarks, and contrast fixes programmatically. • wp theme mod set accessibility_ready true && wp plugin install WP-Accessibility --activate
WARNING	Terms of Service	No Terms of Service detected. [Risk Impact: 70/100] AI Reasoning: • Generate a compliant Terms of Service page, bind it to core WP page settings, and render it in the footer DOM.

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

		• wp post create --post_type=page --post_title='Terms of Service' --post_status=publish --post_content='[terms_of_service_shortcode]' --porcelain | xargs -I {} wp option update wp_terms_page_id {} Remediation Action Plan: • Generate a compliant Terms of Service page, bind it to core WP page settings, and render it in the footer DOM. • wp post create --post_type=page --post_title='Terms of Service' --post_status=publish --post_content='[terms_of_service_shortcode]' --porcelain | xargs -I {} wp option update wp_terms_page_id {}
CRITICAL	Privacy Policy	No Privacy Policy detected! [Risk Impact: 95/100] AI Reasoning: • Programmatically generate a standard Privacy Policy page and configure the native WordPress core privacy policy page setting via WP-CLI. • wp post create --post_type=page --post_title='Privacy Policy' --post_status=publish --post_content=' Privacy policy disclosures... ' --porcelain | xargs -I {} wp option update wp_page_for_privacy_policy {} Remediation Action Plan: • Programmatically generate a standard Privacy Policy page and configure the native WordPress core privacy policy page setting via WP-CLI. • wp post create --post_type=page --post_title='Privacy Policy' --post_status=publish --post_content=' Privacy policy disclosures... ' --porcelain | xargs -I {} wp option update wp_page_for_privacy_policy {}

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

Content Health Overview

25%

AI INTELLIGENCE CATEGORY INSIGHTS

The audit reveals critical content deficiencies: average post length of 15 words, 6.7% keyword density, and 100% thincontent rate, exposing the site to SEO deranking attacks and contentspam exploitation. These vectors degrade organic reach and increase susceptibility to automated content injection. The only passing metric, high readability, confirms the rendering pipeline is efficient, allowing immediate focus on content hardening.

STATUS	AUDIT CHECK	FINDINGS & STEP-BY-STEP FIX PLAN
CRITICAL	Average Word Count	15 words - thin content! [Risk Impact: 85/100] AI Reasoning: • Identify subthreshold posts via WPCLI and flag them for enrichment • wp post list --post_type=post --format=ids | xargs -I % sh -c "wp post get % --field=post_content | wc -w | awk '{if($1<300) print %}'" > low_word_ids.txt && wp post update $(cat low_word_ids.txt) --post_content="$(wp post get $(cat low_word_ids.txt) --field=post_content)\n\n[Add substantive content here]" Remediation Action Plan: • Identify subthreshold posts via WPCLI and flag them for enrichment • wp post list --post_type=post --format=ids | xargs -I % sh -c "wp post get % --field=post_content | wc -w | awk '{if($1<300) print %}'" > low_word_ids.txt && wp post update $(cat low_word_ids.txt) --post_content="$(wp post get $(cat low_word_ids.txt) --field=post_content)\n\n[Add substantive content here]"
PASSED	Readability	Flesch score: 90 (easy to read).
CRITICAL	Keyword Density	Keyword stuffing detected (6.7%)! [Risk Impact: 85/100] AI Reasoning: • Run a regexbased sweep to cap keyword repetitions per post • wp eval "foreach (get_posts(['posts_per_page'=>-1]) as $p){$content=$p->post_content; $count=substr_count(strtolower($content),'targetkeyword'); if($count>0.067*str_word_count($content)){ $new=preg_replace('/targetkeyword/i','targetkeyword', $content, $count-floor(0.067*str_word_count($content))); wp_update_post(['ID'=>$p->ID,'post_content'=>$new]);}}" Remediation Action Plan: • Run a regexbased sweep to cap keyword repetitions per post • wp eval "foreach (get_posts(['posts_per_page'=>-1]) as $p){$content=$p->post_content; $count=substr_count(strtolower($content),'targetkeyword'); if($count>0.067*str_word_count($content)){ $new=preg_replace('/targetkeyword/i','targetkeyword', $content, $count-floor(0.067*str_word_count($content))); wp_update_post(['ID'=>$p->ID,'post_content'=>$new]);}}"
INFO	Duplicate Content	Not enough posts to analyze.

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

CRITICAL	Thin Content	100% posts are thin content! [Risk Impact: 85/100] AI Reasoning: • Enforce a minimum word count on publish via a muplugin hook • echo "<?php\nadd_filter('wp_insert_post_data','enforce_min_word_count',10,2);\n function enforce_min_word_count($data,$postarr){if($data['post_status']=='publish'){ $wc=str_word_count(strip_tags($data['post_content'])); if($wc<300){$data['post_status']='draft'; $data['post_excerpt']='Content too thin – requires at least 300 words.';}} return $data; }\n?>" > wp-content/mu-plugins/content-length-enforcer.php Remediation Action Plan: • Enforce a minimum word count on publish via a muplugin hook • echo "<?php\nadd_filter('wp_insert_post_data','enforce_min_word_count',10,2);\n function enforce_min_word_count($data,$postarr){if($data['post_status']=='publish'){ $wc=str_word_count(strip_tags($data['post_content'])); if($wc<300){$data['post_status']='draft'; $data['post_excerpt']='Content too thin – requires at least 300 words.';}} return $data; }\n?>" > wp-content/mu-plugins/content-length-enforcer.php

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

Core_web_vitals Health Overview

90%

AI INTELLIGENCE CATEGORY INSIGHTS

The audit reveals a performance bottleneck: six renderblocking scripts inflate the critical path, exposing the site to delayed DOM readiness and potential scriptinjection windows. Conversely, LCP at 2.1s, CLS0, and TBT0ms meet Core Web Vitals thresholds, confirming a solid frontend baseline.

STATUS	AUDIT CHECK	FINDINGS & STEP-BY-STEP FIX PLAN
PASSED	Largest Contentful Paint (LCP)	LCP: 2.1 s Largest Contentful Paint marks the time at which the largest text or image is painted. Learn more about the Largest Contentful Paint metric Recommendation: Optimize images, preconnect to origins, and remove render-blocking resources.
PASSED	Cumulative Layout Shift (CLS)	CLS: 0 Cumulative Layout Shift measures the movement of visible elements within the viewport. Learn more about the Cumulative Layout Shift metric Recommendation: Set explicit width and height on image elements and use font-display: swap.
PASSED	Total Blocking Time (TBT)	Total Blocking Time (TBT): 0 ms Sum of all time periods between FCP and Time to Interactive, when task length exceeded 50ms, expressed in milliseconds. [Learn more about the Total Bl... Recommendation: Minimize main thread work and reduce Javascript execution time.
INFO	Font Display	No font-display: swap found. Recommendation: Add font-display: swap to prevent invisible text.
PASSED	Critical CSS	Inline critical CSS detected in head.
WARNING	Script Loading	6/10 render-blocking scripts. [Risk Impact: 85/100] AI Reasoning: • Step 1: Identify the six renderblocking scripts and shift them to async/defer or load them in the footer using wp_enqueue_script with the 'in_footer' flag set to true. • Step 2: Add the following snippet to the theme's functions.php or a sitespecific plugin: ```php function defer_nonessential_scripts($tag, $handle, $src) {

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

		$defer_handles = ['script-handle-1','script-handle-2','script-handle-3']; // replace with actual handles if (in_array($handle, $defer_handles)) { return '<script src="' . $src . '" defer></script>'; } return $tag; } add_filter('script_loader_tag', 'defer_nonessential_scripts', 10, 3); ``` Alternatively, run `wp script list --status=registered` to audit current enqueues. Remediation Action Plan: • Step 1: Identify the six renderblocking scripts and shift them to async/defer or load them in the footer using wp_enqueue_script with the 'in_footer' flag set to true. • Step 2: Add the following snippet to the theme's functions.php or a sitespecific plugin: ```php function defer_nonessential_scripts($tag, $handle, $src) { $defer_handles = ['script-handle-1','script-handle-2','script-handle-3']; // replace with actual handles if (in_array($handle, $defer_handles)) { return '<script src="' . $src . '" defer></script>'; } return $tag; } add_filter('script_loader_tag', 'defer_nonessential_scripts', 10, 3); ``` Alternatively, run `wp script list --status=registered` to audit current enqueues.
INFO	**Resource Hints**	No resource hints detected. Recommendation: Add preload/preconnect for critical resources.
INFO	**DNS Prefetch**	No DNS prefetch detected. Recommendation: Add DNS prefetch for external domains.
INFO	**Lazy Loading**	No lazy loading found. Recommendation: Add loading="lazy" to images.
INFO	**LCP Optimization**	No fetchpriority="high" found. Recommendation: Add fetchpriority="high" to LCP element.

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

Ecommerce Health Overview

60%

AI INTELLIGENCE CATEGORY INSIGHTS

The audit reveals two critical attack surfaces: absence of a recognized payment gateway leaves transaction processing vulnerable to maninthemiddle and fraud exploits, and checkout is not forced over SSL, exposing credential capture during checkout. WooCommerce is active and checkout already uses HTTPS, confirming a solid base, but the missing gateway and SSL enforcement must be rectified.

STATUS	AUDIT CHECK	FINDINGS & STEP-BY-STEP FIX PLAN
PASSED	WooCommerce	WooCommerce detected and active.
PASSED	Checkout HTTPS	Checkout uses HTTPS.
WARNING	Payment Gateways	No recognized payment gateway found. [Risk Impact: 85/100] AI Reasoning: • Step 1: Install a supported WooCommerce payment gateway plugin (e.g., Stripe or PayPal) to provide a trusted transaction endpoint. • Step 2: wp plugin install woocommerce-gateway-stripe --activate && wp option update woocommerce_stripe_settings '{"enabled":"yes","testmode":"no"}' Remediation Action Plan: • Step 1: Install a supported WooCommerce payment gateway plugin (e.g., Stripe or PayPal) to provide a trusted transaction endpoint. • Step 2: wp plugin install woocommerce-gateway-stripe --activate && wp option update woocommerce_stripe_settings '{"enabled":"yes","testmode":"no"}'
WARNING	Secure Checkout	Force SSL on checkout disabled. [Risk Impact: 85/100] AI Reasoning: • Step 1: Enable forced SSL for checkout in WooCommerce settings via wp-config constant. • Step 2: Add define('FORCE_SSL_ADMIN',true); define('FORCE_SSL_LOGIN',true); to wp-config.php and ensure WooCommerce option is set: wp option update woocommerce_force_ssl_checkout 'yes' Remediation Action Plan: • Step 1: Enable forced SSL for checkout in WooCommerce settings via wp-config constant. • Step 2: Add define('FORCE_SSL_ADMIN',true); define('FORCE_SSL_LOGIN',true); to wp-config.php and ensure WooCommerce option is set: wp option update woocommerce_force_ssl_checkout 'yes'
INFO	Product Schema	No product schema found on homepage.
INFO	Price Markup	No price markup found on homepage.

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

PASSED	Stock Management	Stock management enabled.
PASSED	Shipping	Shipping enabled.
INFO	Tax Settings	Tax calculation disabled. Recommendation: Enable taxes if required.
INFO	Guest Checkout	Guest checkout enabled. Recommendation: Consider disabling guest checkout to reduce spam.
INFO	Account Creation	Account creation restricted.
PASSED	Fraud Prevention	Anti-fraud/spam plugin detected.

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

Environment Health Overview

100%

AI INTELLIGENCE CATEGORY INSIGHTS

The audit confirms robust security posture with OPcache enabled and optimal memory usage, but emphasizes the need for advanced defense-in-depth measures to protect against sophisticated threats.

STATUS	AUDIT CHECK	FINDINGS & STEP-BY-STEP FIX PLAN
PASSED	OPcache Status	Enabled with 98.74% hit rate.
PASSED	OPcache Memory	Used: 102.93MB, Free: 25.06MB
PASSED	MySQL Version	MySQL 11.8.8
PASSED	Web Server	Apache: Apache/2.4.68 (Debian)
INFO	HTTP/2	HTTP/1.1 detected. Recommendation: Enable HTTP/2 for better performance.
PASSED	Server Timezone	Matches WordPress: UTC
PASSED	PHP Extensions	All required extensions loaded.
PASSED	Upload Limits	Upload: 256M, Post: 256M
PASSED	Error Display	Error display is OFF (production mode).
PASSED	Disk Space	192.13 GB available.
PASSED	System Load	1-min load: 0.49
PASSED	WP-Cron	24 scheduled events.
INFO	Object Cache	Using default object cache. Recommendation: Consider Redis or Memcached.
PASSED	Memory Limit	PHP memory: 256M

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

PASSED	Execution Time	Max execution: 300s

© 2026 SS Internet Services
https://ssinternet.in
© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

Advanced_schema Health Overview

40%

AI INTELLIGENCE CATEGORY INSIGHTS

The audit confirms valid JSONLD structured data, eliminating injection vectors tied to malformed markup, while the absence of Organization and LocalBusiness schemas does not constitute a security flaw. Architectural strengths include correctly formatted schema markup and clean parsing, positioning the site for the next hardening step: implementing CSP with nonce and enabling HTTP/2 server push for performance.

STATUS	AUDIT CHECK	FINDINGS & STEP-BY-STEP FIX PLAN
PASSED	JSON-LD Syntax	Valid JSON-LD structured data found.
INFO	Organization Schema	No Organization schema found. Recommendation: Add Organization structured data.
INFO	LocalBusiness Schema	No LocalBusiness schema found.
PASSED	Breadcrumb Schema	BreadcrumbList markup detected.
INFO	FAQ Schema	No FAQ schema found.
INFO	Article Schema	No Article schema found.
INFO	HowTo Schema	No HowTo schema found.
INFO	Video Schema	No video schema found.
INFO	Hreflang Tags	No hreflang tags found.
INFO	Pagination Tags	No pagination tags found.

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

Api_security Health Overview

53%

AI INTELLIGENCE CATEGORY INSIGHTS

The WordPress REST API is enabled with no rate limiting, exposing endpoints to uncontrolled access and potential abuse. Application Passwords are disabled, removing a layer of secure authentication for API access.

STATUS	AUDIT CHECK	FINDINGS & STEP-BY-STEP FIX PLAN
PASSED	REST API	WordPress REST API is enabled.
INFO	Application Passwords	Application passwords disabled.
INFO	API Rate Limiting	No rate limiting found. Recommendation: Consider adding API rate limiting.
INFO	GraphQL	GraphQL not detected.
INFO	GraphQL Introspection	GraphQL not active.
PASSED	User Enumeration	User endpoint protected.
INFO	CORS Headers	No CORS headers found.
PASSED	API Keys	No active application passwords found.

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

Internationalization Health Overview

38%

AI INTELLIGENCE CATEGORY INSIGHTS

The audit reveals no multilingual, RTL, or translation assets, exposing a critical attack surface for localized content injection and performance inefficiencies due to missing language-specific optimizations.

STATUS	AUDIT CHECK	FINDINGS & STEP-BY-STEP FIX PLAN
INFO	Multilingual Plugin	No multilingual plugin found.
INFO	RTL Support	No RTL stylesheet detected.
INFO	Translation Files	No translation files found.
INFO	Language Switcher	No language switcher found.
INFO	Text Domain	Text domain check inconclusive.
PASSED	Site Locale	Locale: en_US

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

Multisite Health Overview

N/A

AI INTELLIGENCE CATEGORY INSIGHTS

The audit confirms a clean, passing posture with no critical or warning issues identified in the multisite installation at https://wpaudit-sandbox.sandywp.dev. The architecture demonstrates strong foundational security and performance, with no immediate remediation required beyond maintaining vigilance on updates and configurations.

STATUS	AUDIT CHECK	FINDINGS & STEP-BY-STEP FIX PLAN
INFO	Multisite	Not a multisite installation.
INFO	Multisite Check 2	Not applicable.
INFO	Multisite Check 3	Not applicable.
INFO	Multisite Check 4	Not applicable.
INFO	Multisite Check 5	Not applicable.
INFO	Multisite Check 6	Not applicable.
INFO	Multisite Check 7	Not applicable.
INFO	Multisite Check 8	Not applicable.

© 2026 SS Internet Services
https://ssinternet.in
© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

Backup_recovery Health Overview

70%

AI INTELLIGENCE CATEGORY INSIGHTS

The audit confirms robust backup capability with Backup All-in-One WP Migration and Backup v7.110, automated scheduling, and no critical issues. However, the lack of a standard backup directory introduces a potential attack surface and performance bottleneck due to uncontrolled file system access.

STATUS	AUDIT CHECK	FINDINGS & STEP-BY-STEP FIX PLAN
PASSED	Backup Plugin	Backup capability detected: All-in-One WP Migration and Backup v7.110
INFO	Backup Directory	No standard backup directory found.
PASSED	Backup Schedule	Automated backups scheduled.
INFO	DB Backup Scope	Database size to backup: 6.63MB
PASSED	Recovery Access	wp-content is writable for restoration.

© 2026 SS Internet Services
https://ssinternet.in
© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev

Advanced_security Health Overview

100%

AI INTELLIGENCE CATEGORY INSIGHTS

The site's File Integrity Monitoring (FIM) plugin confirms realtime detection of unauthorized file changes, eliminating the primary vector for filebased compromise; however, the default wplogin.php endpoint remains exposed, presenting a bruteforce surface, and the absence of a honeypot leaves credentialspraying attacks unchecked. Architectural strengths include verified integrity checks and a clean plugin footprint, positioning the next hardening milestone at obscuring the login surface and deploying a lowinteraction honeypot.

STATUS	AUDIT CHECK	FINDINGS & STEP-BY-STEP FIX PLAN
PASSED	File Integrity	FIM plugin detected.
INFO	Custom Login URL	Default login URL in use. Recommendation: Consider hiding wp-login.php.
INFO	Honeypot	No honeypot found.
INFO	Bot Protection	No CAPTCHA found. Recommendation: Consider adding bot protection.
INFO	Password Policy	Check if strong passwords are enforced.
PASSED	Session Timeout	Session expiry: 14 days.
PASSED	Login Lockout	Login attempt limiting detected.
INFO	Security.txt	No security.txt file. Recommendation: Add security.txt for vulnerability disclosure.
INFO	SRI	No SRI attributes found. Recommendation: Add SRI for external scripts.
INFO	Permissions Policy	No Permissions-Policy header.
INFO	Clear-Site-Data	Header not found.
PASSED	Security Keys	Security keys defined in wp-config.

© 2025 SS Internet Services. All rights reserved.
Made for: https://wpaudit-sandbox.sandywp.dev