Sucuri Security – Auditing, Malware Scanner and Security Hardening

By Sucuri

Download

Contributors & Developers

“Sucuri Security – Auditing, Malware Scanner and Security Hardening” has been translated into 14 locales. Thank you to the translators for their contributions.

Translate “Sucuri Security – Auditing, Malware Scanner and Security Hardening” into your language.

Interested in development?

Browse the code, check out the SVN repository, or subscribe to the development log by RSS.

Changelog

2.7.2

- Fix salt bug in the wp-config file.

2.7.1

- Update on the encryption process for the WAF API key due to problems reported on some users.

2.7

- Fixes a lot of readiness warning/errors from PCP.
- Updates how the plugin stores WAF API key.

2.6

- Create new permissions library.
- Fix error causing deletion of WAF API key on clearing cache.

2.5

- Add support for two-factor authentication.

This plugin bundles qrcode-generator (MIT) by Kazuhiko Arase.
Vendored copy due to npm package-injection concerns. We'll switch back to npm when feasible.
Source: https://github.com/kazuhikoarase/qrcode-generator

2.4

- Update list of files to ignore in integrity check.

2.3

- Add theme toggle switch.
- Remove an unnecessary section for users without WAF key.

2.2

- Update integrity section.
- Add a warning when the configured WAF domain does not match site's domain.

2.1

- Fix dark theme conflicting with Woo styles.

2.0

- Added support for WordPress Core vulnerability scanner.
- Added support for PHP vulnerability scanner.
- Added support for plugin's vulnerability scanner.
- Added support for theme's vulnerability scanner.
- Added support for dark theme!

1.9.10

- Fix bug deleting failed logins.
- Fix bug causing WAF blocks due user-agent containing domain names with specific words.

1.9.9

- Fix secret key updater bug: Sometimes API return last character to be "\" breaking configuration file
- Fix Undefined array key "woocommerce_category" PHP warning
- Fix ErrorException caused by stripping all "/" characters from path to htaccess file
- Fix warning caused from malformed path to htaccess file

1.9.8

- Add support for configuration of CORS header

1.9.7

- Add support for configuration of CSP header (report only)

1.9.6

- Added support for filters in the audit logs
- Updated messaging for infected sites

1.9.5

- Updated how the allow PHP files are handled in the integrity tool

1.9.4

- Fixed warning in php 8

1.9.3

- Fixed email notifications error handling

1.9.2

- Improve how the WordPress integrity tool displays added, modified, and removed files

1.9.1

- Add support for configuration of Cache-Control header

1.8.44

- Update Firewall settings page to improve privacy and offer new options to handle API keys

1.8.43

- Update readme and main plugin file to specify license
- Update plugin’s transient name to address to best practices

1.8.42

- Update malware cleanup notification

1.8.41

- Updates navigation to include “More” dropdown
- Add further validation when trying to write HTACCESS

- Update WordPress.org links (redirected from codex)

1.8.40

- Update list of Sucuri cleanup files
- Update successful login screen to show date time

1.8.39

- Fixed API service messaging

1.8.38

- Fixed API service handling when the SUCURISCAN_API_URL config value is not defined
- Fixed API service UI messaging

1.8.37

- Fixed plugin image assets and screenshots to match new branding
- Fixed password reset email link protocol
- Fixed remote fonts usage
- Removed wordpress.sucuri.net API dependency
- Updated screenshots

1.8.36

- Changed Branding fonts, colors and images to match the current Sucuri brand

1.8.35

- Fixed “Early referer checks on admin hooks”

1.8.34

- Added referer check on admin hooks

1.8.33

- Fixed “Added option to clear cache by path”

1.8.32

- Fixed “Empty wp-config file after automatic secret key updates”

1.8.31

- Fixed “Path cannot be empty” error

1.8.30

- Bump version

1.8.29

- Changed ownership

1.8.28

- Silence fopen warning

1.8.27

- Add support for PHP 8
- Reduce memory requirements when reading a log file
- Fix DISALLOW_FILE_EDIT related notice

1.8.26

- Replace the word “blacklist” with “blocklist” in the codebase
- Replace the word “whitelist” with “allowlist” in the codebase

1.8.25

- Fix notice about MONTH_IN_SECONDS in WP < 4.4
- Update reset password workflow

1.8.24

- Fix warning caused by humanTime function
- Fix fatal error caused by cron jobs with nested arguments

1.8.23

- Add Automatic Secret Keys Updater
- Improve button's and link's messaging on Last Logins sections
- Improve messaging on Hardening page
- Improve messaging on IP Access page

1.8.22

- Add "SSL existence check" to WordPress Security Recommendations
- Add "Salt & Security Keys existence check" to WordPress Security Recommendations
- Add "Salt & Security Keys age check" to WordPress Security Recommendations
- Add "Admin account check" to WordPress Security Recommendations
- Add "Single super-admin check" to WordPress Security Recommendations
- Add "Too many plugins check" to WordPress Security Recommendations
- Add "File editing check" to WordPress Security Recommendations
- Add "WordPress debug check" to WordPress Security Recommendations
- Add "Basic hardening check" to WordPress Security Recommendations
- Add a delete button on Last Logins sections
- Add register of logs removal on Audit Logs
- Fix display of Access File Integrity on NGINX/IIS servers
- Remove PHP version check from hardening page

1.8.21

- Add WordPress Security Recommendations section in the dashboard
- Add PHP version check
- Fix goo.gl links
- Fix post_type pattern match to allow numbers and max of 20 chars
- Fix Audit Logs queue timezone issue
- Fix regex in template string replacement
- Update translation file to include WordPress Security Recommendations section fields
- Make the menu icon use the menu color styling

- Remove block button from failed logins page

1.8.20

- Add dynamic core directories in the hardening allowlist options
- Modify scheduled tasks panel to load the table via Ajax
- Allow hosting details display to be filterable
- Preparation for translations

1.8.19

- Add option to refresh the SiteCheck malware scan results
- Add support for a CLI command to ignore files in the core integrity check
- Fix text

1.8.18

- Keep settings when the plugin is deactivated, unless the plugin is uninstalled

1.8.17

- Update Terms of Service and Privacy Policy

1.8.15

- Make default plugin options filterable
- Fix missing button to manually activate the advanced features
- Remove unnecessary tags from README per WordPress guidelines
- Modify resolution of the images to respect retina display

1.8.14

- Add filter to allow automatic configuration of the settings

1.8.13

- Add new version of the GPL v2 license file

- Remove unused option to reduce number of failed logins
- Fix multiple typos in the code found after a diff parse
- Modify name of the base library file for consistency
- Modify wording of the API key panel in the settings page
- Add option to include the hostname in the alert subject
- Fix open_basedir restriction was not considered on scans
- Remove firewall API key deletion on re-authentication

1.8.12

- Fix invalid array when deselecting all security alerts
- Add language files to the list of ignored changes
- Modify internal response to the log file not found error
- Add option to force the firewall cache flush
- Fix unexpected exception when open_basedir is in place
- Add support to export and import trusted IP addresses
- Add link to the audit logs API endpoint for developers
- Add reverse ip address in all email alerts from visitor
- Remove API key from the settings that can be exported
- Modify code to make default plugin options filterable
- Add ability to store the settings in the object cache
- Add support for wp-cli and command to generate an API key
- Fix missing documentation tags in the command line library
- Fix format and coding standard in CSS and JavaScript files
- Add button to toggle the visibility of the post-types table
- Modify order of the added, modified, removed core files
- Fix relative file path when ABSPATH is point to root
- Add additional notifications for changes on users

1.8.11

- Modify Sucuri firewall detection with regular expressions
- Modify option to force scanner to ignore directories
- Modify form to monitor and ignore post-types
- Modify miscellaneous changes in some alert messages
- Modify error message displaying for invalid CSRF validations
- Fix minor issues with the version detection code
- Remove internationalization support for consistency

- Add support for the RTL reading direction
- Add API key in admin notice when it is being deleted
- Fix modification date for corrupt core files
- Fix audit log parser for incompatible JSON data
- Fix password visibility when the option is changed

1.8.10

- Version bump skipped

1.8.9

- Remove duplicated failed user authentication log
- Remove trailing forward slash from asset URL
- Fix post-type ignore tool to allow hyphens in the ID
- Fix queries to the database in the last logins page
- Remove unnecessary option queries to the database
- Fix PHP notice for a string offset cast occurred
- Remove unnecessary data from the website info page
- Modify timing for the execution of the Ajax requests

1.8.8

- Add smart limit to send logs from the queue to the API
- Add option to ignore events for post transitions
- Fix infinite loop with email alerts and SMTP plugin
- Add option to configure the malware scanner target URL
- Add option to enable the auto clear cache firewall function
- Modify status of the directory hardening using the Firewall
- Modify error message in audit logs when the API key is missing
- Modify timing for the dashboard alerts after an update
- Modify firewall clear cache button to execute via Ajax
- Modify firewall settings page to load data via Ajax
- Add option to blocklist IP addresses with the Firewall API
- Fix order of the audit logs when the queue is merged
- Add more directories to ignore during the scans
- Add option to customize the URL for the malware scans
- Fix error interception for Firewall API errors

- Add support for other English and Spanish based languages
- Modify mechanism to ignore files from integrity checks
- Add option to stop sending the failed login passwords
- Modify default value for some of the alert settings
- Remove unnecessary statistics panel for the audit logs
- Modify output for the malware results to simplify links
- Add option to override the timezone for the datetime
- Add option to configure the WordPress checksums API
- Add maximum execution time avoidance in the integrity tool
- Add support to run diff on deleted WordPress files

1.8.7

- Fix multiple issues with the API calls
- Add queue system to fix website performance
- Fix non-dismissable newsletter invitation message
- Fix performance of the audit log parser without regexp
- Add conditional to check for the availability of SPL
- Add cache for the audit logs to make dashboard responsive
- Modify frequency of the file system scans to run daily
- Remove option to configure the maximum API timeout
- Modify location of the scanner options and scheduled tasks
- Add button to send the logs from the queue to the API

1.8.6

- Add default language for internationalization fallback

1.8.5

- Fix minor bugs after post-testing of the new release
- Add full support for internationalization with en_US locale
- Add full support for internationalization with es_ES locale

1.8.4

- Modify the entire interface to offer a fresh design
- Add support for internationalization via gettext

- Modify the structure of the project for maintainability
- Remove minified files to facilitate future contributions
- Add warning message in the reset plugin tool page
- Fix loading sequence for additional PHP files
- Add restriction to prevent direct access to PHP files
- Fix file search by name when the directory is passed
- Add HTTP request parameters to track some settings
- Fix reset plugin tool with the new WordPress API
- Fix length of the pagination helper with many pages
- Add performance boost for the failed logins page
- Modify structure of the failed logins data analyzer
- Fix deactivation of all the scheduled tasks from settings
- Modify entire code base to enforce HTTPS over HTTP
- Remove heartbeat settings after performance improvement
- Remove unnecessary XHR event monitor and report
- Remove deprecated functions from previous releases
- Remove deprecated tool to scan for error_log files
- Modify failed logins logger with wrong passwords
- Remove plugin checksum dependency to avoid asset cache
- Modify minimum PHP version in hardening page
- Fix email alerts with non-existing site_url option
- Add tool to import and export the plugin settings
- Add uninstall instructions during deactivation of the plugin
- Fix plugin reinstall procedure with backup and prechecks
- Modify mechanism to ignore irrelevant WordPress core files
- Modify list of available scheduled task frequencies
- Fix lazy load of the CSS and Scripts on the correct pages
- Add audit log message fixer for the wpephpcompat_jobs event
- Fix website URL in the template for the email alerts
- Add message in the core integrity tool for false positives
- Add option to reset the content of some storage files
- Add mechanism to display self-hosting logs as fallback
- Fix incoherent failed login processor on pagination
- Add option to display differences in core integrity checks
- Modify the default and maximum timeout for the API
- Fix static data storage path to allow server migrations
- Add option to ignore non-registered custom post-types
- Add more details into the event that monitors post deletions

- Fix event monitor for plugin activation and deactivation
- Fix dynamic directory tree deletion with improved performance
- Fix automatic deletion of conflicting plugins
- Add event monitor for all supported post status transitions
- Add one-time newsletter invitation after plugin updates
- Add code to delete legacy plugin options from database
- Modify error on non-processed files in the integrity checks
- Fix overflow of HTTP requests to SiteCheck API on failures
- Fix handling of the actions in the core integrity checks
- Add message and button to reset the audit logs cache
- Add ajax request to load malware scans for performance

1.8.3

- Removed goo.gl links
- Fixed fatal error when PHPMailer failed
- Fixed incorrect selected value in settings
- Added SiteCheck for arbitrary domain
- Various code cleanup

1.8.2

- Modified logic of the settings in database checker
- Modified default value for the available updates alerts
- Fixed undefined array and object keys in audit logs
- Fixed incompatibilities with foreign API service responses
- Added development option to keep using the database
- Added panel with information about the plugin settings
- Added conditional to prevent redeclaration of class
- Fixed cache flush method used to delete datastore

1.8.1

- Modified default setting for the core integrity alerts
- Added more files to the core integrity ignore list
- Fixed support for custom data storage directory
- Fixed admin notices after changing alert settings
- Fixed settings and audit logs for the firewall page

- Fixed regression with clear cache in firewall page

1.8.0

- Added error message when storage is not writable
- Fixed option getter to migrate plugin settings if possible
- Fixed base directory name without PHP **DIR** constant
- Fixed user authentication denial when no blocked users
- Fixed htaccess standard rules checker with no WP_Rewrite

1.7.19

- Added method to rescue HTTP requests using sockets
- Fixed mishandled JSON data in audit logs Ajax request
- Modified list of firewall features and promo video

1.7.18

- Added options library using external file instead of the database
- Modified API calls using custom HTTP request using Curl
- Fixed core files marked as broken in a Windows server
- Fixed pagination links in last and failed logins page
- Fixed password with ampersands in email alert
- Fixed allowlist hardening using the authz_core module
- Removed unnecessary emails to reduce spam
- Added constant to stop execution of admin init hooks
- Added explanation for invalid emails and no MX records
- Added link to open the form to insert the API key manually
- Added more options in the IP discoverer setting
- Added option to configure malware scanner timeout
- Added option to configure the API communication protocol
- Added option to reset the malware scanner cache
- Added scheduled task and email alert for available updates
- Added tool to block user accounts from attempting a login
- Added tool to debug HTTP requests to the API services
- Various minor adjustments and fixes

1.7.17

- Added API service failback mechanism
- Added core integrity email on force scan
- Slight interface redesign
- Various bugfixes and improvements

1.7.16

- Fixing a low severity XSS (needs admin access to create it)

1.7.14

- Added alternative method to send email alerts
- Added button to reset options with explanation
- Added suggestion for new users to check plugin settings
- Allow mark as fixed non-writable core files
- Fixed display menus items single or network panels
- Fixed handle boolean values in PHP config retrieval
- Fixed non-standard content location in core integrity
- Fixed user identifier as integer on password reset
- Modified css and js files to reduce size
- Modified do not load resources on hidden sidebar
- Modified fully redesign of general settings page
- Modified hide update warning if versions are the same
- Modified wording of post-types alert settings
- Removed ellipsis of long IPv6 addresses in last logins
- Removed unnecessary dns lookups in infosys page
- Removed unnecessary monospace fonts in settings status
- Removed unnecessary ssl verification option processor

1.7.13

- Fixed issue affecting site performance
- Fixed clear hardening of previous versions
- Modified report and block non-processable ajax actions
- Added configure DNS lookups for reverse proxy detection
- Added option to configure comment monitor and logs
- Added option to configure the XHR monitor and logs

1.7.12

- Improved hardening options
- Added more logging events
- Various bugfixes and improvements

1.7.11

- Reverted change for firewall detection to protect legacy users

1.7.10

- Added better checks for SSL issues
- Fix for audit log timezones
- Various bugfixes and improvements

1.7.9

- Improved reinstallation process
- Updated sidebar banners
- Various bugfixes and improvements

1.7.8

- Fixed bug on the secret keys hardening.

1.7.7

- Added better support for directory separators
- Added option to remove API key from plugin
- Various bugfixes and improvements

1.7.6

- Added audit log reporting.
- Added more settings for better control.
- Added support for more actions.

- Improved multisite support.
- Added support for reverse proxies.
- Various bugfixes and improvements.

1.7.5

- Added better handling of API responses of remote scanner.

1.7.4

- Added option for keeping failed logins until the user removes them.
- Bugfixes for user reported issues.

1.7.3

- Error log panel.
- Various bug fixes.

1.7.2

- Messaging and FAQ updates.

1.7.1

- Fixed remote scanning that was not loading automatically on some installs.

1.7.0

- Added Hardening option to remove error log files
- Bug fixes on some new registrations.
- Changed format of the internal logs to json.

1.6.9

- Multiple bug fixes (as reported on the support forums).
- Added heartbeat for the file scans.
- Code cleanup.

1.6.8

- Fixing interface.

1.6.7

- Added Support for integrity checks on i18n installations.
- Fixed the setting change bug.

1.6.6

- Internal code cleanup and re-organization.
- More white lists for the integrity checks.
- Additional settings to customize some of the warnings.

1.6.5

- Fixed integrity checking display.

1.6.4

- Fixed API generation bug.

1.6.3

- Added proper brute force alerts.
- Added option to restrict number of emails.
- Added more description to the emails.
- Added a list of failed login attempts inside the last login tab.

1.6.2

- Setting a maximum number of emails per hour.
- Fixing typos.

1.6.1

- Initial release with new auditing options.

1.6.0

- A new dashboard to welcome users to the new features of the plugin.
- Overall design of the interface of all the pages were modified.
- SiteCheck scanner results were filled with more information.
- SiteCheck scanner results markers when the site is infected/clean.
- System Info page were simplified with tabulation containers.
- Integrity check for administrator accounts was optimized.
- Integrity check for outdated plugins/themes was optimized and merged.
- IPv6 support in last logins statistics.

1.5.7

- WordPress 3.9 compatibility

1.5.6

- Added IPv6 support.
- Fixed links and messaging.

1.5.5

- Added list of logged in users.
- Added system page.
- Change the integrity checking to use WP API.

1.5.4

- Bug fixes.

1.5.2

- Adding additional information about .htaccess hacks and the server environment.

1.5.0

- Fixing last login and giving better warns on permission errors.
- Making the integrity check messages more clear.

1.4.8

- New and clean design for the scan results.
- Adding a web firewall check on our hardening page.

1.4.7

- Cleaning up the code a bit.
- Only displaying last login messages to admin users.
- Storing the logs into a log file instead of the db.

1.4.6

- Increasing last login table to the last 100 entries.

1.4.5

- Fixing some issues on the last login and allowing the option to disable it.

1.4.4

- Small bug fixes + forcing a re-scan on every scan attempt (not using the cache anymore).

1.4.3

- Fixing a few PHP warnings.

1.4.2

- Fixing a few PHP warnings.

1.4.1

- Small bug fixes.

- Adding last IP to the last login page.

1.4

- Added post-hack options (reset all passwords).
- Added last-login.
- Added more hardening and the option to revert any hardening done.

1.3

- Removed some PHP warnings and code clean up.
- Added WordPress integrity checks.
- Added plugin/theme/user checks.

1.2.2

- Tested on WP 3.5.1

1.2.1

- Tested on WP 3.5-RC4
- Style changes

1.2

- Cleared PHP warnings
- Added /inc directory
- Added /lib directory
- Logo added
- Default stylesheet added
- Header area added
- Sidebar area added
- Restyled 1-click hardening page
- Removed old malware page

1.1.7

- Tested on WP 3.5-RC3.

1.1.6

- Upgrading for WP 3.3.

1.1.5

- Removed PHP warnings / code cleaning.

1.1.3

- Cleaning up the results.
- Added 1-click hardening.

1.1.2

- First release that is good to be used (debugging code removed).

1.1.1

- First public release.

Version	2.7.2
Last updated	6 days ago
Active installations	600,000+
WordPress version	3.6 or higher
Tested up to	6.9.4
Languages	See all 15
Tags	firewall malware scan security spam

Advanced View

Ratings

4.2 out of 5 stars.

5 stars		285
4 stars		21
3 stars		9
2 stars		4
1 star		64

Your review See all

Contributors

Sucuri

Support

Issues resolved in last two months:

1 out of 5

View support forum

Donate

Would you like to support the advancement of this plugin?

Donate to this plugin