Centrora Documentation

Release 1.0.0

Centrora

Dec 06, 2017

About

The documentation for Centrora Security is organized into a couple of sections as follows. A simple text version in PDF can be downloaded at here.

CHAPTER 1

About Centrora Security

Centrora Security is an all-in-one system providing the overall security solutions for the websites. It includes the Virus Scanner, Firewall, and Backup Tool, with the built-in schedule management offering a high level of automation. Our mission is to take the stress out of website security for our customers so they can focus on running their businesses.

We help business of all sizes with:

WordPress & Joomla Modules

Easy to download modules for WordPress and Joomla websites.

High Security Online Protection

Basic free protection services through to premium services at a great price.

Free Malware Removal

A free malware removal service on websites for all annual subscribers

Cyber Crime Info and What To Do

Regular information on what you can do to protect yourself from cyber crime.

CHAPTER 2

Changelog

7.0.2

- Minor bug fixes for firewall scanner v7.
- Minor bug fixes for core directory scanner.
- Added new hash files.
- Added missing language tags.
- Fixed Wordpress centrora security badge.
- Fixed cron job page to include git backup pre-requisite checks only when the user want to change the scheduled git backup settings.
- Added new OEM.
- Fixed links to update the plugin version

7.0.1

- Fixed missing v7 firewall file issue

7.0.0

- Added new feature: new improved, faster and efficient Firewall v7 scanner.
- Use of high speed dedicated servers for virus scanning and Git backups.
- Removal of classic backup.
- Improved Git Backup which supports increased cloud backup space of 10 GB.
- Improved the feature to update the virus and firewall patterns.
- Improved efficiency of MD5 hash scanner, core directory scanner, vulnerability scanner and file permission scanner.
- Improved manual and schedule scanning.
- Minor bug fixes for Firewall scanner V6.

6.6.4.1

- Fixed: download function not working on some websites
- Fixed: PHP errors in php7.1.1
- Improved Email templates

6.6.4

- Added WordPress 4.7.1 and 4.7.2 hash files for core file scanning

6.6.3

- Updated email templates
- Improved virus scanning functions
- Improved firewall scanning functions when variables are iterated arrays

6.6.2

- Update Mailer class to remove Joomla version codes

6.6.1

- Remove PHPmailer and use Default WordPress PHPmailer to send emails

6.6.0

- Added new OEM
- Improved UI for all scanner sections
- Fixed Firewall Scanner bug when variable is an nested array
- Updated software update url to github url
- Fixed virus scanner bug for whitelisted files
- Plesk Panel support
- Update PHP Mailer to latest version

6.5.16

- Added WordPress 4.7 hashes files

6.5.15

- Fixed mark as clean doesn't work correctly on schedule scanning issues

6.5.14

- Added WordPress 4.6.1 hashes for Core Directory Scanner

6.5.13

- Updated Backup function to check file permissions before performing actual backup

6.5.12

- Fixed minor warning errors when checking URLs for cronjob requests

6.5.11

- Fixed installer not working on Windows server due to the lack of INNODB engine

6.5.10

- Updated API IP address

6.5.9

- Improved Add IP function to cleanup IP title to enhance security, credits to 'Plugin Vulnerabilities'

6.5.8

- Add administrator checking to improve AJAX security check function to enhance CSRF protection

6.5.7

- Improved AJAX security check function to enhance CSRF protection

6.5.6

- Fixed update error for French language websites

6.5.5

- Added French language package

6.5.4

- Fixed span tags not showing properly in malware detail popup
- Added French language support preparation package

6.5.3

- Added background scanning function

6.5.2

- Improved Malware scanner function
- Improved Database installation function to reduce database connections
- Added WordPress 4.5.3 hashes

6.5.1

- Improved Marked As Clean function in Virus scanner

6.5.0

- PHP 7 support
- Improved the efficiency of schedule virus scanner to
- Improved the efficiency of Gitbackup

6.4.3

- Improved Git Backup for large websites
- Fixed other minor UI bugs

6.4.2

- Fixed Git push to cloud name error

6.4.1

- Fixed Git push to cloud error

6.4.0

- Improved Gitbackup function
- Improved Gitbackup UI
- Improved Gitbackup cronjob

- Disable google bot user agent detect
- Improved: import csv file function in IP Management section
- Fixed: Scan result status filter not working properly on some websites
- Added WordPress 4.5.1 and 4.5.2 hash files

6.3.5

- Fix free virus scanning function not working properly on some servers

6.3.4

- Improved Gitbackup checking function

6.3.3

- Improved Virus Scanning report section UI

6.3.2

- Fixed IP import function not working properly when CSV file is modified in Windows Excel file
- Added IPv6 Support
- Improved Virus Scanning report section UI
- Improved firewall scanning report email by adding the link to the IP information page

6.3.1

- Fixed the blank header section in the configuration page
- Fixed some minor css issues.
- Fixed the scan report result link to the scan report in the WordPress version for Joomla versions

6.3.0

- Improve Cloud backup for Gitbackup
- Improve dynamic Virus scanner UI
- Added new schedule scanner function
- Fixed firewall rules update function not working on some servers
- Fixed Core directory scanner not working on some servers

6.2.4

- Fixed some css and javascript issues in the dashboard and Gitbackup UI

6.2.3

- Close error display

6.2.2

- Fixed error handling function not working properly on some servers for Gitbackup

6.2.1

- Added Git Backup error handling message if Git is not installed
- Added Git Backup folder protection

6.2.0

- Added Git Backup

- Improved User Interface

6.1.4

- Fixed IP Import not functioning after security token method is changed

6.1.3

- Fixed IP cannot be added and virus scanner cannot start for some websites after the token method changes

6.1.2

- Fixed IP curb and scanning report not showing up properly issues after the token method changes

6.1.1

- Fixed a low severity XSS vulnerability in backup file name function, credits to Erin Germ
- Fixed a low ot medium severity CSRF vulnerability when an article is posted by Editors with the form to manipulate the Centrora database, credits to Erin Germ

6.1.0

- Updated Core Directory Scanner
- Add more hashes for Joomla and WordPress previous versions

6.0.7

- Updated WordPress hash for 4.4.2

6.0.6

- Fixed bugs for Windows server
- Fixed directories not showing correctly in WHM installation for Core directory scanning
- Remove the scanning of Long queries (more than 255 characters)
- Fixed Vulnerabilities scanner showing com_contact as vulnerable for Joomla 3.4

6.0.5

- Fixed virus scanning report reloading to the 1st page if the current page is not in the 1st page

6.0.4

- Fixed scheduled virus scanner not working on some servers

6.0.3

- Fixed modified file scanner not working issue on some websites
- Fixed virus scanner report csv file not working properly on WordPress websites
- Fixed email template not showing properly when the save button is clicked the from the second time

6.0.2

- Harden the website by adding one rule to prevent remote execution vulnerability
- Fixed PHP notice message for advance firewall scanner
- Add Joomla remote code execution vulnerability protection
- Fixed virus scanner notice warnings
- Add function to block IPs with malicious user agents
- Add function to block IPs with fake google bots

- Updated Email template editing function

6.0.1

- Added more rules in checking malicious user agent
- Removed Google Authentication in Block page when the option is turned off
- Updated mail class
- Fixed configuration setting not saved successfully on some servers

6.0.0

- Added: Brand New Look and feel! – We took valuable feedback from you our customers and revamped the look of Centrora Security. Give it a go, we think you will love it!
- Added: Help text to give users a better understanding of each configuration setting
- Added: Strong Password Enforcement under Firewall configuration settings
- Added: A What's New section where you can view News of security and other related posts from our own security consultants – learn what you can do to harden your site's security
- Enhancement: Merge Firewall Configuration Functions
- Enhancement: Improved firewall configuration settings layout – Rearranged & simplified configuration settings
- Enhancement: Reduced duplicate functions under Firewall
- Enhancement: Improved site navigation speed
- Enhancement: Changelog view under what's new to get details of each release

5.0.8

- Enhancement: Improve file upload function to have better user experience

5.0.7

- Enhancement: Hide errors for all situations
- Enhancement: Add extra protection on data folder

5.0.6

- Fixed: Language file not loaded properly for scheduled virus scanning.

5.0.5

- Fixed: The syntax for OEM version does not work in PHP version 5.3 that caused some websites not working properly
- Added: Administrator URL protection for both WordPress, Joomla and Suite versions
- Added: Security Manager Account management section to add a security manager account to manage Centrora Security
- Enhancement: Enhanced CSS and UI support for OEM partners
- Added: Security warning message in configuration page to enable the Centrora System plugin for Joomla and Suite users
- Bug fixed: Suite version only – fixed errors showing in the administrator menus
- Bug fixed: Suite version only – JFactory not found error when loading the language tags

5.0.4

- Added: Added file upload logging function for premium users

- Enhancement: Enhanced the panel for allowed file extensions for file uploads

5.0.3

- Fixed: Fixed the Firewall checking warning message shows incorrectly when the firewall is turned on

5.0.2

- Enhancement: Improve the virus scanner and scanner report to use stricter patterns to avoid false alerts

5.0.1

- Enhancement: Change the virus scanner to use stricter patterns during the scanning to avoid false alerts

5.0.0

- Added: Brand New Look and feel! – We took valuable feedback from you our customers and revamped the look of Centrora Security. Give it a go, we think you will love it!
- Added: Help text to give users a better understanding of each configuration setting
- Added: Strong Password Enforcement under Firewall configuration settings
- Added: A What's New section where you can view News of security and other related posts from our own security consultants – learn what you can do to harden your site's security
- Enhancement: Merge Firewall Configuration Functions
- Enhancement: Improved firewall configuration settings layout – Rearranged & simplified configuration settings
- Enhancement: Reduced duplicate functions under Firewall
- Enhancement: Improved site navigation speed
- Enhancement: Changelog view under what's new to get details of each release
- Enhancement: Improved Dashboard design (Phase 1) – expect more to come!
- Fixed: Audit page fixes to "Fix" button
- Fixed: Other minor visual bug fixes
- Fixed: Minor JS fixes for data pagination

4.9.4

- Enhancement: improve firewall scanner to avoid an warning error when returning scanning results
- Enhancement: improve virus scanner to detect PHP injection scripts faster

4.9.3

- Fixed: Fixed firewall version not updated when using the Update Signature function
- Fixed: Fixed virus Pattern update was not successful for some servers when using the Update Virus Pattern function

4.9.2

- Enhancement: Improved the returned message after the firewall signature is updated.

4.9.1

- Fixed: Fixed the signature update function in Advance Firewall Panel
- Fixed: Fixed backup panel not showing up properly in some servers with PHP version lower than 5.4
- Fixed: Minor fix for Javascript functions
- Updated: updated the Danish language file

4.9.0

- Added: Add Google Drive backup
- Added: Feature Requests #91: Back up function Offer other Options for Low server memory constraint users
- Added: Support for larger file size uploads (cloud backup)
- Added: Feature Requests #124: Add manual update function in the admin backend
- Added: Feature Requests #167: Add download virus pattern function to virus scanner section
- Enhancement: Improved backup Upload time – Faster More efficient Cloud Backups.
- Enhancement: Split backups for manageable file sizes
- Enhancement: Backup option for timeout constraint servers (during files backup)
- : Improvements #119: Reorganise Menu System for better navigability
- Fix: Scheduled backup function fixes
- Fix: Bugs #85: Creating Backup Zip fails for some users
- Fix: Bugs #127: Premium Subscription multisite login Issues
- Fix: Bugs #161: Email template mass
- Fix: Minor UI fixes
- Fixed: Fixed warning error: "Undefined property: stdClass::$ischecked in fwscanner.php"

4.8.5

- Fixed: Fixed Quarantine file failed issue in Joomla component version

4.8.4

- Fixed: Ban IP page css not loaded properly for some websites

4.8.3

- Fixed: duplicated IP in IP management

4.8.2

- Enhancement: Improved firewall scanner class to remove miscellaneous warning errors
- Enhancement: Improved firewall management codes to avoid duplicated IP showing in the IP management section
- Enhancement: Added variable validation function on backup path variable in backup management section
- Enhancement: Improved Dropbox and One Drive Authentication function

4.8.1

- Fixed: Schedule Tasks hour selector saving the wrong time on the server.
- Added: Added email template restore function.

4.8.0

- Added: New and Improved Schedule Task: Set and forget, get notified,
- Added: Feature Requests #120: Scheduled backup function
- Added: Feature Requests #123: Add Ondrive backup
- Added: Feature Requests #130: WooCommerce Support on Variables Scanner

- Added: Feature Requests #137: ADD OEM Login Page
- Enhancement: Cloud backup folder structure now includes better support for multiple sites backup
- Enhancement: Schedule Scanner minor UI Improvements
- Enhancement: Save backup time of new backups made
- Enhancement: Schedule Task toggle Activate/Deactivate
- Enhancement: Improvements #121: Dashboard Links to Data
- Enhancement: Numerous other minor Enhancements and fixes
- Enhancement: Improvements #126: curb Session: Login Status
- Fixed: Schedule Scanner failed for a few users
- Fixed: Bugs #122: Dashboard popup error, on low resource servers.
- Fixed: Bugs #125: Dropbox Unlink Account Fails to Relink later
- Fixed: Bugs #129: Fix Audit my Site broken actions
- Fixed: Bugs #132: Fix CronJobs Msg: Link for "contact support team" in WP
- Fixed: Bugs #142: Virus Scanner Maximum Database connection saving error
- Fixed: Several minor tweaks and fixes

4.7.1

- Enhancement: Improve the IP Mask function in the Add IP Form
- Fixed: Some whitelisted variables are still being scanned in Basic Firewall
- Fixed: Fixed 'PhpmailerException' class redeclaration issue

4.7.0

- Added: Feature Requests #87: Add self unblock support
- Added: Feature Requests #90: OEM user access curb
- Added: Feature Requests #92: Ability to edit alert notification email template
- Enhancement: Improvements #96: For admin to receive emails, adding the domain in the email so the administrator knows which domain the attack is from
- Enhancement: Improvements #97: Add units on traffic map and fix Facebook like box errors
- Enhancement: Improvements #106: Improve the block page layout and design
- Enhancement: Improvements #108: Only send email out when the domains are matched in the attack
- Enhancement: Improvements #115: Log in page improvement and bug fix
- Fixed: Bugs #89: Virus Scanner Cronjob Stops
- Fixed: Bugs #93: Language codes missing in Admin email panel
- Fixed: Bugs #102: IP address not showing correctly when suite installed on Mac
- Fixed: Bugs #109: Windows server support (from Scott)
- Fixed: Bugs #110: Subscription Logout 500 Internal Server Error
- Fixed: Subscription checkout JQuery tag
- Fixed: Various other minor bug fixes and improvements

4.6.2

- Fixed: Fixed Windows server cannot add IP into the database issue – Credits to Scott Berry (www.processingpoint.com) to report this issue
- Fixed: Fixed IP cannot be added into the IP Management panel when there is a 0 on the left side of each part of the IP address

4.6.1

- Enhancement: Improve file permissions and virus scanner custom scanning directory function
- Fixed: Fix premium service page cannot login issue

4.6.0

- Added: Feature Requests #7: Dropbox Backup
- Added: Feature Requests #14: More functions in Scan Report
- Added: Feature Requests #71: Add a filter into the IP management section to filter IPs for specific type of variable
- Added: Feature Requests #84: Add directory tree map into the virus scanner
- Added: Feature Requests #86: Add a function to insert the oem customer id into the Configuration table
- Added: Feature Requests #90: OEM user access curb
- Enhancement: Added the direct access link to the IP address that is reported as spammers by the spammer detection function.
- Enhancement: Improvements #76: Add Subscription modal to the premium service
- Fixed: Bugs #45: Export IP to CSV
- Fixed: Bugs #46: Geo Data progress bar goes beyond 100%
- Fixed: Bugs #69: Foreign Language not showing properly
- Fixed: Bugs #73: Virus scanner cannot complete virus scanning
- Fixed: Bugs #88: Suite Administrator Menu Visual Bug
- Fixed: Bugs #95: Cannot add domains in Administrator Management

4.5.2

- Fixed: fixed ajax action 'addorder' and 'getPaymentAddress' not added into the ajax library for the subscription controller

4.5.1

- Minor Enhancement: improve new email notification function to increase efficiency
- Minor Enhancement: improve updater to update to 4.5.0

4.5.0

- Fixed: Bugs #15: IP management some flags are missing for some websites
- Fixed: Bugs #53: Fix variable cannot be added to suite / joomla in some websites
- Fixed: Bugs #55: In a specific website website, the variable Whitelist not working
- Fixed: Bugs #56: In a specific website, the OSE Security Suite cannot upgrade to Centrora Security Suite
- Fixed: Bugs#57: In a specific website, user cannot login premium service
- Fixed: Bugs#63: In a specific website, Virus scanner cannot complete virus scanning

- Added: Feature Requests #16: Add an email notification when the backup is completed
- Added: Feature Requests #24: Add One Click fix for file permissions functions
- Added: Feature Requests #44: Add multiple email alert receivers facilities
- Added: Feature Requests #49: Add landing page to show all features for the premium service
- Added: Feature Requests #72: Add database version to ensure smooth database updates
- Added: PDO class activation codes in the php.ini activation section for suite version
- Enhancement: UI #50: Change the one column login UI to two columns UI
- Enhancement: UI #51: Add a button to the activate my premium page to smooth premium service activation
- Fixed: Bugs #15: IP management some flags are missing for some websites
- Fixed: Bugs #53: Fix variable cannot be added to suite / joomla in some websites
- Fixed: Bugs #55: In a specific website website, the variable Whitelist not working
- Fixed: Bugs #56: In a specific website, the OSE Security Suite cannot upgrade to Centrora Security Suite
- Fixed: Bugs#57: In a specific website, user cannot login premium service
- Fixed: Bugs#63: In a specific website, Virus scanner cannot complete virus scanning

4.4.0

- Added: Backup function for database and files for the whole WordPress and Joomla website
- Added: File permission function to change the file permissions of the system
- Added: Added email for the virus scanning cronjob when the scanning is completed
- Fixed: In Windows server, the IP cannot be added into the database
- Fixed: Virus Cronjob cannot be completed in some servers

4.3.8

- Fixed: Scanning specific path not working properly on some servers

4.3.7

- Enhancement: adjusted maximum threshold function to block an IP address so it will block the IP once it exceeds the threshold instead of blocking the IP in the next time
- Added: Added single thread scanning function so the scanning can be performed on some servers with strict database connection requirements.
- Added: Backup, Clean, Delete function in scanning report
- Fixed: Scanning specific path not working properly on some servers
- Fixed: Fixed Autoloader not working when the firewall is activated globally in the php environment where local php configuration is not allowed

4.3.6

- Enhancement: Improved virus scanner
- Added: Added CURL method to download the update package
- Added: Added Backup, Clean, Backup Clean function for virus scanning report
- Added: Added Activation with Activation code function for premium services

4.3.5

- Added: Added highlight of the virus scanner report
- Enhancement: Enhance the firewall function to ignore json format request variables

4.3.4

- Enhancement: Forced display_errors to be disabled when running the Centrora Firewall for all instances
- Enhancement: MainWP Extension to support some commercial MainWP addons

4.3.3

- Enhancement: Improved MainWP Extension so it checks if the extension is enabled in the Child websites

4.3.2

- Enhancement: Changed MainWP Class loaded inside wordpress backend

4.3.1

- Enhancement: Improved virus scanner so it can scan a larger amount of files in the system
- Enhancement: Improved virus scanner for cronjob virus scanning functions
- Enhancement: Minor CSS style improvement to enhance the UI
- Added: Added MainWP Extensions Support

Fixed: Fixed the Composer class has been declared in some Joomla websites

4.3.0

- Enhancement: Improved user interface
- Added: Cron job for virus scanning (automatic daily virus scanning)

4.2.2

- Enhancement: Separate the Firewall Configuration Page and the Firewall Rules Fine-tuning page
- Enhancement: Added explanations of each ruleset in the basic firewall to let customers know more about the how Centrora Security

4.2.1

- Fixed: Custom Ban Page cannot be saved successfully on some servers.
- Added: Added version check and plugin update function

4.2.0

- Fixed: Mailer not sending email correctly when SMTP is on
- Fixed: Login panel not working when in Security Suite mode for Joomla websites
- Added: Added Custom Redirection function for users who has a custom ban page
- Fixed: Fixed Warning Errors in Anti-Spamming function
- Fixed: Fixed the email notification being sent even the Configuration Option 'Receive Centrora Firewall / SafeBrowsing Update Email' is set to Off

4.1.8

- Fixed: Fixed warning error reported by AlanP57: Undefined index: option in wp-content/plugins/ose-firewall/vendor/oseframework/wordpress.php on line 50

4.1.7

- Enhancement: Further Improved Anti-Spam function for registration form which blocks the spammer directly

4.1.6

- Added: Added Anti-Spam function for registration form

4.1.5

- Fixed: Fixed Configuration Window being covered by the left administrator menu in WordPress CMS – Credits to Tina Granzo (www.citybeautifuldesign.com)
- Fixed: Fixed typo error in Virus Scanner panel – Credits to Tina Granzo (www.citybeautifuldesign.com)
- Fixed: Fixed typo error in .htaccess activation codes
- Enhancement: Further Improved Alert Email

4.1.4

- Improved: Improved Alert Email
- Fixed: Fixed Virus Scanner cannot be loaded in Google Chrome in some servers

4.1.3

- Improved: Further Improve virus scanner to avoid server timeout issue for some resources limited servers

4.1.2

- Improved: Improve virus scanner to avoid server timeout issue for some resources limited servers

4.1.1

- Improved: Improve respond actions for virus scanner to handle network error
- Improved: Added restrictions on SQL user connection for Virus scanner, so it will queue until the connection is released to avoid heavy mysql server load
- Improved: Improved language tags in the virus scanner
- Improved: Improved Development mode detection function to avoid errors for some servers

4.1.0

- Added: Added rule to protect WordPress Admin Ajax file being attacked by LFI attack
- Improved: Improved Dashboard layout

4.0.9

- Improved: Improved security badge widget
- Added: Added Badge Status Checking in Audit panel

4.0.8

- Added: Added Safe Browsing Checking Information table in Audit panel
- Added: Affiliate Tracking Code Input Form in Audit Panel
- Fixed: Administrator email address not show up correctly in Firewall Configuration form.

4.0.7

- Added: Added System Pre-requisites check before framework is loaded

4.0.6

- Added: Add debug mode to avoid exception handler catch global errors

4.0.5

- Enhancement: Improve javascript for account validation function in the login panel

4.0.4

- Fixed: Fixed dashboard not Javascript function not correctly in Google Chrome version 39.0.2171.65
- Fixed: Fixed Google 2-Step Verification Configuration not showing correctly in version 4.0

4.0.3

- Enhancement: Improved scanning class to harden protection and avoid IP spoofing
- Enhancement: Improved dashboard section to avoid CSRF attack
- Fixed: Fixed error warning for WordPress website with lower version

4.0.2

- Added: Added PHP version to check ensure the PHP version (5.3.0) requirement is fulfilled.

4.0.1

- Fixed: Account action not loaded properly in My Premium Service Panel

4.0.0

- Enhancement: Completely rewrite User Interface which is fully responsive
- Enhancement: Completely rewrite framework to reduce database connection and memory usage
- Enhancement: Completely rewrite framework to enhance efficiency in detecting hacking attempts
- Enhancement: New virus scanning architect to simultaneously scan all types of viruses in the server which makes the scanning faster and consume less CPU sources

3.8.4

- Fixed: Fixed incorrect database export download link issue

3.8.3

- Fixed: Fixed database export download link returns 0 issue.
- Enhancement: Enhance the virus scanning function to ignore the parent path of scanning path

3.8.2

- Fixed: Fixed a bug caused by the conflict setting in Country blocking and Basic Firewall configuration

3.8.1

- Fixed: Fixed database table cannot be created in WordPress4.0
- Fixed: Fixed database table cannot be created (duplicate key error) when the database of the WordPress installation is shared with other WordPress installation

3.8.0

- Fixed: Fixed session error when the WordPress is integrating with Magento
- Enhancement: Improved virus scanner class to avoid multiple process being created
- Added: Added dropbox backup function in backup section

3.7.2

- Fixed: Fixed the ip2long function overflow issue for 32bit servers
- Enhancement: Improved the manage IP javascript functions

3.7.1

- Added: Added Custom Scanning Path in Virus Scanning section

3.7.0

- Added: Added Export IP function in the IP Management Section
- Enhancement: Add page size and sorting filters in the country section

3.6.6

- Enhancement: Improve database class to reduce database connections
- Enhancement: Improve backup page interface
- Enhancement: Improve Converter function to work with array variables
- Enhancement: Improve IP block function to fit with the scanning result in SQL Inject Me Firefox Addon

3.6.5

- Enhancement: Improve the IP Management Grid so the title and IPs can be copied
- Enhancement: Added Schedule Virus Scanning function for Premium service users

3.6.4

- Fixed: Fixed virus version not showing correctly issue in the Virus Scanning section

3.6.3

- Enhancement: Added advanced virus patterns in virus scanning section

3.6.2

- Enhancement: Added the page size alternation field in the IP management panel
- Enhancement: Added the function to close the SafeBrowsing window
- Enhancement: Added the data reload function for the order ascending / descending field
- Enhancement: Improved the javascript to be compatible with the https protocol
- Enhancement: Improved the variable filter function for Advanced Firewall function

3.6.1

- Enhancement: Added sorting filter and page size field in the IP Management Panel
- Enhancement: Added database object closure in the firewall scanning object to reduce redundant database connections
- Enhancement: Updated Advanced Firewall Version

3.6.0

- Fixed: Fixed the Daily Audit Report not sending out on some servers bug
- Enhancement: Added PHP Configuration Audit in Daily Audit Report

3.5.9

- Fixed: Fixed the Basic Rule title not showing correctly in the basic firewall rules section
- Enhancement: Improved the receive Centrora Firewall email function for premium service
- Enhancement: Improved the convertVariables function to convert variables when they are array
- Enhancement: Added the check Database ready function to the badge widget to avoid errors
- Enhancement: Added the PHP configuration checking in the Daily Audit Report
- Enhancement: Added PHP security enhancement function in the configuration section

3.5.8

- Fixed: Fixed the index undefined warning error in the getDisableFunctions function in Audit class

3.5.7

- Enhancement: Updated the email function to reduce duplicated emails being sent when an attack is found
- Enhancement: Updated all files to add 'Direct access denied' function to enhance security
- Enhancement: Extended the time difference for the safe browsing status checking
- Fixed: No sender information in the alert email when attack is detected
- Added: Added the Change All Country function into the Country Block page
- Added: Added the receive Centrora Firewall email option in the scanning configuration
- Fixed: Fixed the multiple countries status change function not working correctly in Country Block Page.
- Enhancement: Improved Scanning Configuration layout
- Added: Added PHP Configuration Auditing function to enhance overall security

3.5.6

- Fixed: Fixed configuration page not showing correctly on non-English websites
- Fixed: Fixed records cannot be deleted issues in Admin-Email Mapping section

3.5.5

- Added: Added API Configuration View in Configuration section.

3.5.4

- Added: Added option to turn on and off Daily Audit report
- Updated: Updated the firewall rules version
- Fixed: Fixed a minor warning bug in the installer for checking country database
- Fixed: Fixed a minor warning bug in the getSafeBrowsingStatus function in the Audit class
- Enhancement: Improved the virus scanning function to reduce overall memory usage
- Enhancement: Improved Configuration model to avoid warning errors in PHP strict mode
- Enhancement: Improved CountryBlock model to avoid warning errors in PHP strict mode
- Enhancement: Improved CountryBlock class to reduce duplicated download of SQL files if it has been downloaded
- Enhancement: Improved Variable function to work with both Joomla and WordPress
- Enhancement: Improved ClamD class to avoid warning errors in PHP strict mode
- Enhancement: Improved Firewall Statistics class to work with both Joomla and WordPress
- Enhancement: Improved getSafeBrowsingStatus function to avoid warning errors in PHP strict mode
- Removed: API Key in configuration section depreciated since this version.

3.5.3

- Fixed: Remove old url and Update url links in the firewall badge
- Added: Added safebrowsing checkup function in dashboard
- Updated: Updated the remote login class to allow automatic status update for premium service users

- Fixed: Fixed development mode auditing function bug

3.5.2

- Fixed: Removed WordPress version in the signature checking function in the audit class
- Fixed: Minor bug: the getConfiguration by type function has an error in the SQL query in the statistic class
- Enhancement: Added Subscription plans and enhanced checkout procedure in advanced firewall setting section

3.5.1

- Fixed: Blank Dashboard page due to table not installed
- Added: Added daily audit report to inform administrators about the status of the security status of the website.

3.5.0

- Added: Added the Get Advance Firewall Rules function into the Advance Firewall Dashboard
- Added: Added the daily automatic update of firewall rules in the advanced firewall section
- Added: Added the daily automatic update notification for firewall rules in order to notify administrators about the updates
- Fixed: Wrong help link in the scanning report page

3.4.2

- Added: Add back API field in the configuration section for some users to test the API function.

3.4.1

- Updated: Update the Local File Inclusion rule to reduce false alert

3.4.0

- Fixed: Removed views from the database that caused the database backup and restore interruption
- Enhancement: Updated database uninstallation function to clear all Centrora tables

3.3.1

- Fixed: On some servers, the virus type table interrupts the installation process
- Fixed: Token missed in the database uninstallation page.

3.3.0

- Security Enhancement: Anti-CSRF checking for all admin tasks, credits to Juan Manuel Fernández (juanma@quantika14.com)

3.2.1

- Added: Pattern and Pattern ID in Scanning Report

3.2.0

- Removed: Advanced Firewall setting panel
- Removed: Advanced Firewall checking in Dashboard Panel
- Fixed: Google Authenticator function keeps showing disabled even it is enabled in Dashboard
- Added: Country Blocking Panel and Download function
- Added: ClamAV integration into the Virus Scanning Function

3.1.3

- Fixed: IP cannot be deleted in the IP Management Panel

3.1.2

- Removed: Removed the installation of views in the database
- Fixed: Fixed the configuration cannot be saved in windows server
- Fixed: Fixed virus scanner cannot work on Windows server
- Added: Change username for the 'admin' account in Dashboard

3.1.1

- Enhancement: Change some wording in the dashboard to clarify the meaning of the menus
- Enhancement: Add 'fix it' button at the end of every warning bar.

3.1.0

- Enhancement: Enhance dashboard layout
- Enhancement: Removed unnecessary database connections
- Added: About page to show all short links to the pages in the plugin
- Enhancement: Change the remote login function to fit Centrora Panel 1.0.7

3.0.7

- Enhancement: Use the default WordPress Contact email address in the ban page instead of the default value created in the Centrora SQL file
- Removed: removed the duplicated createTable.sql file in the data folder

3.0.6

- Fixed: On some servers, the auto loader function cause blank screen.
- Fixed: On some servers, the PDO connection exceeds the maximum number of connection configured in MySQL setting. Adding datanbase connection closing codes to resolve it.

3.0.5

- Enhancement: Added the version number in the dashboard
- Enhancement: Updated the remoteLogin class to work with Centrora Panel 1.0.5
- Fixed: On some websites, the administrator's email cannot show up in the Admin-Email Mapping Panel

3.0.4

- Fixed: On some websites, the checking of Development mode causes a blank screen
- Fixed: Missing closing tag for the warning message for development checking
- Enhancement: Warning message style improved
- Enhancement: Clarified warning message for the advance firewall setting

3.0.3

- Fixed: On some websites, the administrator's email cannot show up in the Admin-Email Mapping Panel
- Fixed: Ajax class missed the ORequest Class when Centrora Panel calls the functions in the class
- Enhancement: Added a function to check if allow_url_fopen is turned on for a website
- Enhancement: Added a function to check if Development mode is turned on for the website
- Enhancement: Added a function to check if the advanced firewall setting is turned on for the website
- Enhancement: Removed duplicated 'Advanced Firewall' field in the scanning configuration panel

3.0.2

- Enhancement: Improved Dashboard Layout to have more user friendly navigation
- Enhancement: Improved Configuration Layout to have clearer navigation for functions like advanced firewall setting, country block and Google Authenticator
- Enhancement: Checked if the user has used other Google Authenticator plugin than Centrora Google Authenticator before loading the Google Authenticator plugin
- Enhancement: Remove the permission denied message for Country Block Page

3.0.1

- Enhancement: Removed the secret word wording from scanning configuration page
- New: Added Advance Firewall Setting function

3.0.0

- Enhancement: Improved Backend User Interface
- Enhancement: Re-designed Virus Scanning Engine, virus scanner is now 20x faster
- Enhancement: Improved Backend User Interface
- New: Added Database Backup function
- New: Central Security Management Integration with Centrora Panel
- New: Added File Upload Scanning function
- New: Added Google Authenticator (2 step authentication) function

2.2.6

- Fixed: temporarily fix the admin-email mapping not being able to fix in Google Chrome browser
- Fixed: fixed the 'Constant OSEAPPDIR already defined' error
- Enhancement: Enhance the YiiBase library to avoid open_basedir curb for the library autoload function

2.2.5

- Fixed: further fix for some websites the administrator lists cannot be shown in the Admin-Email Mapping section.

2.2.4

- Fixed: admin-email mapping delete function not working in some servers because the JSON encoded ID value is escaped
- Fixed: admin-email mapping add linkage function showing incorrect return message even the linkage was added successfully

2.2.3

- Fixed the admin-email mapping controller for the incorrect return messages for the Ajax message box.

2.2.2

- Fixed some websites the administrator lists cannot be shown in the Admin-Email Mapping section.

2.2.1

- Enhancement: Remove the HTML Purifier auto register function in order to solve the 500 error issue in some server.

2.2.0

- Enhancement: Added menu bar into the curb panel for easy navigation
- Enhancement: Improved firewall statistic library to reduce PHP warning errors
- Enhancement: Improved virus scanner library to reduce PHP warning errors
- Enhancement: Improved oseAjax class to support Joomla CMS
- Enhancement: Improved oseDatabase class to support Joomla CMS
- Enhancement: Improved oseEmail class to support Joomla CMS
- Enhancement: Improved oseInstaller class to support Joomla CMS
- Enhancement: Improved oseRequest class to support Joomla CMS

2.1.4

- Enhancement: Improved Germany Language Translation. Credits to Alexander Pfabel
- Enhancement: Added the debug mode option in the configuration panel to turn off error displaying function in the frontend. Credits to Wombat

2.1.3

- Enhancement: Added the function to check if the curl_exec is enabled for a hosting account, if so, the Stop Forum Spam function will be disabled.
- Enhancement: Improve the backend css file to adjust the font-size to match default wordpress font-size. Credits to Alexander Pfabel
- Enhancement: Improve the badge seal layout and background images

2.1.2

- Enhancement: Added Germany Support – credits to: German translation by Alexander Pfabel (http://alexander.pfabel.de)
- Fixed no data issue in Admin Email Mapping config page, Credits to shadowood, and itpixie
- Enhancement: make the Admin Email Mapping Editing window closable

2.1.1

- Add back i18n multiple language solution library, some environment requires this. Credits to joedeagnon

2.1.0

- Significantly reduce package size
- Fixed Class 'CHtmlPurifier' not found error during database creation section. Credits to mikeotgaar
- Fixed wrong warning message shown in Variables management. Credits to shadowood, and kamill
- Fixed Virus Scanner Panel: no progression bar during scan. Credits to shadowood
- Fixed Virus Scanner Panel: no progression bar during scan. Credits to shadowood
- Fixed incorrect format for option 'File Extensions' in the virus scan config page. Credits to shadowood
- Fixed incorrect sizing for scan file size box. Credits to shadowood
- Enhancement: remove GeoIP database tables requirements, significantly reducing Database size. . Credits to shadowood

2.0.2

- Remove Secret Word Descriptions
- Fixed non-English website not able to load javascript language files issues

2.0.1

- Fixed Badge update issue
- Fixed Virus database update issue
- Fixed Database keeps display not ready issue

2.0.0

- Improved front-end protect seal showing function
- Rewrite the whole plugin to implement the MVC structure

1.6.4

- Improved front-end protect seal showing function
- Improved front-end protect seal CSS style

1.6.3

- Fixed the log table not created properly issues on some servers

1.6.2

- Fixed a typo in the security seal

1.6.1

- Updated Chinese and Germany languages, credits to Mr Alexander Pfabel
- Fixed the Class 'osewpScanEngine' not found issue for some servers

1.6.0

- Added Stop Forum Spam Anti-spamming checking, keep your blog spam free
- Added Security Protection Badge, shows the confidence of your website security to your clients
- Added the logs of virus scanning to show the scanning records in the security protection badge

1.5.4

- Removed duplicated menus as suggested by Lime Canvas (https://wordpress.org/support/profile/limecanvas)
- Fixed the issue where OSE Firewall Settings links are appended to all plugins links section (credits to Lime Canvas https://wordpress.org/support/profile/limecanvas)
- Fixed the wpdb undefined issue when initializing file list into the database

1.5.3

- Updated the codes to make it work with multiple websites (credits to scottnath, https://wordpress.org/support/profile/scottnath)
- Improved function to check admin accounts
- Fixed PHP warning errors for undefined OSE Firewall setting variables

1.5.2

- Updated Chinese and Germany languages, credits to Mr Alexander Pfabel

1.5.1

- Fixed back-end admin menu causing warning message issues (reported by mike http://www.graphicline.co.za/ and Alan https://wordpress.org/support/profile/alanpae, AlanP57 https://wordpress.org/support/profile/alanp57)
- Fixed language file loading error issue (credits to scottnath, https://wordpress.org/support/profile/scottnath)

- Fixed redirection function error issue reported by numzi https://wordpress.org/support/profile/nunzi
- Avoid scanning back-end blog post action to avoid false alerts with javascript codes inserted in to blog posts (thanks for the report by Alexander https://wordpress.org/support/profile/herzwacht and

1.5.0

- Added four protection modes: OSE Firewall only, OSE Security Suite only, OSE Firewall plus OSE Security Suite and Development mode (protection temporarily turned off)
- Added a server IP field to avoid false alerts due to empty user agent
- Fixed the field 'Detect Directory Traversal' not being saved properly issue
- Added custom banning message field and custom banning message function
- Enhance OSE Banning page appearance
- Enhance Javascript injection detection pattern to avoid false alerts
- Added OSE Virus / Malicious codes scanning function

1.0.2

- Added Germany Translation language
- Added the maximum tolerance parameter, so the attacker will be blocked automatically after X times of attack

1.0.1

- Added French Translation language

1.0.0

- Initial release

CHAPTER 3

Prerequisites

Centrora Security requires,

1. PHP version 5.4+.
2. MySQL 5.0+.
3. WordPress 4.7+.
4. All Joomla! versions 1.5, 2.5, and 3.x.
5. Git Backup function requires Git installed on the server.

CHAPTER 4

Install on WordPress Site

Step 1.

Please go to WordPress admin section –> `Plugins`, and click the `Add New` button.

Step 2. Search for "Centrora" in the search panel. `Install` it after finding Centrora plugin.

Step 3.

After the installation completes, click on the `Activate` button to activate the plugin. A new plugin "Centrora Security" will be added to the WordPress side panel.

Step 4. Enter Centrora main panel and go to the menu `Management` –> `Install/Uninstall`. Click the `Install Database Tables` button to finalise the installation.

Now Centrora Security is ready to use and we can start the configurations.

Manually Install Centrora Plugin on Wordpress. If you have troubles in intalling it from WrodPress using the above method, please try the manual way to install it. Please refer to the video. Manually Install Centrora on WordPress

CHAPTER 5

Install/Update on Joomla! Website

The installation of Centrora plugin in a Joomla! website is quite easy. Please follow the below steps. The method also works to update Centrora to the latest version when you already have Centrora installed.

Step 1.

Go to Joomla! administration installation page through Joomla! back-end –> menu `Extensions` –> `Manage` –> `Install`. Then go to the tab `Install from URL`.

Step 2.

Simply copy/paste the URL into the box:

```
https://github.com/Centrora/centrora-joomla/archive/master.zip
```

and click `Check and Install` button.

Step 3.

After we get the installation success message, let's go to the menu `Components` –> `Centrora Security` to enter Centrora. On Centrora Panel, we need to install the database at `Management` –> `Install/Uninstall` for the first time installation.

Step 4. Also, please make sure the Centrora System system plugin is enabled. You can enable it by clicking the `Fix it` button if you see the notice message in the above Management menu. Or you can go to Joomla! Plugins Management, Joomla! `Extensions` –> `Plugins` and search for "Centrora". Enable it.

Congratulations!. Now the installation is done and we can continue the configurations.

5.1 Alternative Installation Method

If you have any troubles installing it using the above way, like the failed connection to our server or memory limit, please try the manual way to install it.

1. Download the install package to your computer from your account section on our website or the direct link, Centrora Joomla! Package

2. Extract the package “centrora-joomla-master.zip” on your computer.
3. After the extraction, you can get a folder “packages” and find two packs in the folder “plg_system_centrora.zip” and “com_centrora.zip”.
4. Further, extract the pack “com_centrora.zip” on local and upload all files to the website `/site_root/tmp/centrora` folder through the FTP.
5. Install it in Joomla! `Extensions` –> `Install` –> `Install from Folder` and enter the absolute path of the above upload directory to the box.
6. Click `Check and Install` to start the installation.
7. Do the same steps for the pack “plg_system_centrora.zip”.
8. Now it’s done and please follow the previous Step 3 and Step 4 to finalize the installation.

Please don’t hesitate to contact us if there is still any problem there.

CHAPTER 6

Activate Premium Functions

We strongly recommend you to subscribe to our Premium Service to enjoy Centrora Security's much-extended range of functions and services.

First, after the Centrora Security installation, please go to the menu `My Premium`.

Step 1. If you have had an account with Centrora, please login directly at the left panel. If you don't have an account yet, please create a new one using the form at the right side or you can register the account on our website www.centrora.com. Then please login in Centrora with the new account.

Step 2. After the login, all licenses in your account will be listed. Please use the button `Activate` to link the license to the website. It will automatically activate all premium functions and services in the current Centrora installation.

Step 3. If you don't have any licenses yet or all licenses have been used up, you might need to get more licenses. Please choose the proper license package in the store of Centrora website. After the subscription, please return to you Centrora `My Premium` and refresh the page. Licenses will show up and please follow the Step 2 above to activate the premium service.

Now you have the premium service activated and all functions and features have been available. Please note, each centrora installation needs a separate license, therefore, if you have more installations of Centrora, you will need more licenses to activate the premium service for them all.

CHAPTER 7

Uninstall Centrora from the System

In case that you want to thoroughly remove Centrora System from your site or server, please follow the steps below.

7.1 WordPress Version:

1. Remove the tables and data from the database first in `Centrora --> Management → Install/Uninstall`.
2. Disable it in WordPress Plugins.
3. Remove it.

7.2 Joomla! Version:

1. Remove the tables and data from the database first in `Centrora --> Management → Install/Uninstall`.
2. Disable the Centrora plugin is Joomla! Plugins manager.
3. Uninstall the component `OSE Firewall` and plugin `Centrora` in Joomla! Extensions Management.

7.3 Centrora Suite Version:

1. Remove the tables and data from the database first in `Centrora --> Management → Install/Uninstall`.
2. Deactivate the protection for your site by removing the activation codes from the .htaccess. php.ini, or index.php file. It depends on in which way you did the protection activation at the beginning.
3. Remove the Centrora folder from the server.
4. Remove the database for the Centrora installation in MySQL.

CHAPTER 8

Dynamic Scanner and Virus Cleaning

Centrora Security system integrates a Virus Scanner - Online Anti-Virus tool for scanning and cleaning the website which has been compromised. Currently, the scanner is available for Free users, however, the detailed scan result and cleaning tools are only available for Premium Subscribers. Also, please note that the scanner only scans the file system but not the database.

Please refer to the video for How to do a quick dynamic scan for the website. Do A Dynamic Scan for the website Also, watch the video for how to review the scan result and clean the files. How to Review the Scan Result and Clean the Files

Or, please follow the below steps in details to do a full website scan.

8.1 1. Dynamic Scanner

Let's start a scan now. please go to the menu `Search for Malware` → `Dynamic Scanner`. It will show the main operation panel of the scanner.

8.2 2. Configurations

First, please configure file extensions, maximum file size, etc for the scan in the button `Config Setup`. The unit for file size is MB. `Maximum Database Connection` is an advanced parameter. If you know the DB connection limit on your server, please set the parameter accordingly; and please set it as 100 if you have no idea about it. For the `Max Execution Time`, we recommend setting it as 300.

8.3 3. Scan Types

Select Scan Types to choose what types of virus you are going to scan. Generally, if you have no idea about it, please just choose `Deep Scan` to do a full scan.

8.4 4. Start a Scan

Now we can start a scan. By simply clicking the `START` button, it will do a full website scan.

If you just want to scan a specific target or some folder outside of the current website root, you can use `Scan Specific Folder` to choose the folder or define the path to scan.

1. Click the small folder icon to extend the sub-folders/files tree under the folder.
2. Please note that if you enter the path value manually, it requires the absolute path.
3. Click the button to start the scan.

8.5 5. Scan Progress

During the scan, the main panel will show the progress and also the status of the server memory and CPU usage. You can use `STOP` button to cease the process and then use "Continue" button to re-start it from the previous stop point. After the scan completes, it will give a brief scan result.

8.6 6. Scan Result

Now we can view the scan result in the menu `Search for Malware` → `Scan Result`. It is highly recommended that before you clean or quarantine any of the reported files, double-check whether they are truly infected with the virus or false positives. It's because that Virus Scanner might occasionally trigger false alerts on some legitimate files. Clicking on View and checking the file codes manually can reduce the possibility of falsely deleting any system core files.

After clicking the View button, the Scanner will pop out a window to show the file source codes and also highlight the codes that are recognised as malware.

8.7 7. Cleaning Options

We have some optional Actions to deal with the files after reviewing the codes.

1. `Clean` - We can choose to clean the highlighted suspicious codes if the codes are just injected into a functional file. Use the **Clean** button on the code viewing window or after selecting the file in the scan result panel.
2. `Quarantine` - Alternatively, if you find that all the codes in the file are malware codes, please **Quarantine** the file entirely because the file could be uploaded by the hacker.
3. `Mark as Clean` - If you think it's a false alert, you can **Mark as Clean** to whitelist it.
4. `Restore` - Also, if you find the website doesn't run correctly after you clean or quarantine some file, you can use **Restore** button to restore it to the original copy before the operation.
5. `Manually Clean` - If you find that the Scanner only marks the key patterns of the virus, rather than highlighting all the codes infected, the file needs to be cleaned manually. You need to do this via an FTP or the File Manager in your Host Control Panel.

8.8 8. Export Scan Report

After checking all files, you might do a scan again to verify if the website is clean. Before that, you can export the current scan/cleaning logs to a .csv file for the future reference. Simply click Export to CSV button and save the file to your PC.

Despite our best efforts to keep updating the Scanner (online anti-virus), it might still be unable to recognise some specific infections. In some case, some virus evolves, or the hacker alters the way they encode the virus codes. Therefore, if you believe the Scanner cannot detect all the virus files on your site, or the site still encounters problems after you clean it, please don't hesitate to contact our Support Centre. We will arrange developers to do the check for you.

CHAPTER 9

Other Scanning Tools

Besides the core Dynamic Scanner, Centrora Security system also integrates some other scan tool which can assist us to thoroughly clean the website and to confirm if the website has been fixed.

9.1 Core Directories Scanner

Core Directories Scanner will scan the website to compare the core system files with the original official package. Just click `Start Scanning` inthe menu `Search for Malware --> Core Directories Scanner` to do the scan. After a scan, it will report the files which are modified, removed, and suspicious compared to the original version. Take a Joomla! site as an example,

Note: The result is just for the reference. It doesn't mean that the files listed in the result are the malware files. It's because site may have 3rd party extensions and libraries installed. So please review the files briefly to have more information. Or please contact us for help.

9.2 Modified File Scanner

Sometimes, the Dynamic Scanner cannot finds all virus files on the sites, for example:

1. The hacker uploads the hacking files in a package and not all files there contains the virus patterns;
2. The files are encoded in a special way to hide from the scanner.

In this case, the Modified File Scanner may help which can show the files modified within a time range which we can define. For example, if we think the site was hacked on date X or we find some suspicious files with the date X, we can use Modified File Scanner to find out all files changed around date X, say (X-3, X+3). Then we can get all files which could be involved in the hacking.

Go to the menu `Search for Malware --> Modified File Scanner`, define the date range and the scan path. Then `Start scanning`.

9.3 MD5 Hash Scanner

MD5 Hash Scanner will scan the file MD5 Hash of the core system files to report the suspicions. Please update MD5 Hash database before the scan.

CHAPTER 10

Useful Techniques

Even we update the Virus signature every day, there could still be new virus variations or codes which are encoded in a special way by hackers. The Scanner may not be able to pick out all malware files efficiently. If we find the website keeps getting problems like being frequently hacked or sending spam emails after you have cleaned the site, we need to use some techniques to find our the hidden codes in the website. Here we introduce some useful ones.

10.1 Track the File/Directory Change Time

We sometimes observe that some specific files/directories keep being hacked. There is always because there are hidden codes in the website or some extensions have vulnerabilities. In this case, we need to find our the codes location which hack the know files.

First, we need to know the **exact date/time** of the file being modified. Please note this it not the modified time which we can find through the FTP. It's because the hacking codes may be able to change the file modified date shown in FTP to hide the useful information.

Then, we can check the **server raw access logs** for the records around the above exact change time to find our what files/commands did it.

10.1.1 Case 1: the specific file keeps being hacked.

We need to get a notification when the file is hacked again and we use the script to achieve this. For example, the file is at `/home/xxx/public_html/test.php`. Clean the file first. Then we get the latest modified date/time of the file by run a PHP file containing the codes:

```
<?php
  $time = filemtime("/home/xxx/public_html/test.php");
  echo $time;
?>
```

Run the file to get the time value, say `1491806973`.

Create another PHP file `modified.php` and place the codes in it:

```
<?php
  //#Check the modified date/time of the file:
  // File
  $file = "/home/xxx/public_html/test.php";
  $time = filemtime($file);
  if ($time != '1491806973')
  {
    $result = mail("sample@domain.com","File hacked","File changed again"."\nFile␣
↪time: ".date("Y-m-d H:i:s", $time)."\nEmail time: ".date("Y-m-d H:i:s"));
    echo "Completed-".$result."<br>";
  }
?>
```

Here, replace `sample@domain.com` to your own email address.

Now, add the script `modified.php` to the server cron job to make it run every 3 minutes:

```
wget -q -O /dev/null http://your_domain/modified.php
```

When it detects the file is changed again, it will send an notification to your email where the "Email time" is the latest changed time. If you want the script to stop running whenever it detects any change to reduce the duplicate emails, please rename the file after `echo "Completed-".$result."<br>";` with the codes to make it:

```
echo "Completed-".$result."<br>";
rename ("/home/xxx/public_html/modified.php" , "/home/xxx/public_html/modified.php.bk
↪");
```

We can check the server raw logs around that time to find more useful information.

10.1.2 Case 2: a specific folder always has strange uploaded files.

In this case, we need to know the time when the files are really uploaded. We will count the file number in the folder, keep monitoring the number and send notification when the number changes.

Run the below script the count the current file number of the clean folder:

```
<?php
  // Directory
  $directory = '/home/xxx/public_html/test';
  // Returns array of files
  $files = scandir($directory);
  $count = count($files);
  echo $count;
?>
```

Say the number of files is 9. Create the new PHP file `count.php` as:

```
<?php
  //#Check the change of file count of a directory:
  // Directory
  $directory = "/home/xxx/public_html/test";
  // Returns array of files
  $files = scandir($directory);
  $count = count($files);
  if ($count != 9)
  {
    $result = mail("sample@domain.com","File added","Directory changed again"."\nFile␣
↪time: ".date("Y-m-d H:i:s", $time)."\nEmail time: ".date("Y-m-d H:i:s"));
```

```
    echo "Completed-".$result."<br>";
    rename ("/home/xxx/public_html/count.php" , "/home/xx/public_html/count.php.bk");
  }
?>
```

Replace `sample@domain.com` to your own email address.

Add the script `count.php` to the server cron job to make it run every 3 minutes:

```
wget -q -O /dev/null http://your_domain/count.php
```

When new files are uploaded to the folder, it will detect the change and sen the notification with the time. We can check the server logs to find out the location of the hidden uploader.

10.2 Find File Sending Emails

We might observe spam emails are sending from our server. However, it's very hard to locate the scripts which send them. Here we can have a method to track their locations if we can define a local PHP configuration on the server.

First, we need to define these 2 parameters in the PHP configuration. For example, on your server, the websites is located in the directory `/home/doamin/public_html`, define:

```
mail.add_x_header = On
mail.log = /home/doamin/public_html/phpmail.log
```

It could be a php.ini file on your server. Please make sure it's the loaded PHP configuration of all scripts on the server.

Then we can do a test. Upload a `test.php` to the site `/tmp` directory. Add the PHP codes to the file:

```
<?php
// the message
$msg = "First line of email body\nSecond line of email body";

// use wordwrap() if lines are longer than 70 characters
$msg = wordwrap($msg,70);

// send email
mail("Jack@test.com","Test Email",$msg);
?>
```

Run the test file at *http://your_site_domain/tmp/test.php*. If the email is sent, it will be logged in the `phpmail.log` file which we defined previously:

```
[06-Oct-2016 01:38:43 America/Chicago] mail() on [/home/domain/public_html/tmp/test.
↪php:9]: To: Jack@test.com -- Headers:
```

Here we can find the file location which sends the email. After setting all these, we can check the mail log file next day. We can then know all files sending emails during the period.

CHAPTER 11

Configure Firewall Settings of Centrora Version 6

11.1 Enable Centrora Firewall

Now, we can turn On Centrora Firewall to protect the website from attacks. Go to the menu `Firewall Settings --> Firewall Configuration`, under the tab `Firewall Scanning`, turn on `firewall`. Setting it off will disable the Firewall scanning functions temporarily for the development purpose.

Also, if you have Premium activated, please further go to the tab `Advanced Firewall Configuration` to enable `Advanced Firewall Setting` and `Silent Mode`. The Advanced Firewall Setting is the switch of the advanced functions and features. It has more secured patterns and rules to help preventing all aspects of XSS attacks, sql injection etc. It will be only available for paid premium subscribers.

11.2 Frontend Blocking Mode

1. There are 2 modes here. With **Show ban page**, if the user's behavior violates any rule, the user's IP will be thoroughly blocked and they will receive a Ban Page which you can edit below.
2. The **Show a 403 error page** function allows a certain user's activity to be filtered, but the user's IP will not be blocked and will just receive a 403 error page. Afterwards, the user can still get back to the site.

Note: We will recommend the mode of **Show a 403 error page**, in case the Firewall triggers false alerts. Banning the visitors' IPs may frustrate legitimate users.

---

3. **Silent Mode** in the `Advanced Firewall Configuration` is also recommended. It works with the v mode above. Under this mode, if an activity is recognized as hacking by Anti-Hacker, the user will be redirected to the URL with the suspicious string trimmed. Though the IP will not be blocked it will have been added to the monitored IP list. Thus, users will not be confused when their operations are falsely recognised as hacking activities.
4. Even under the mode of **Show a 403 error page**, we have the option to block the IP which keeps violates the rules and is considered belonging to a real hacker. **Silent Mode Allowed Threshold** in the `Advanced`

`Firewall Configuration` defines the max number of suspicious visits of an IP. The default value is "10".

11.3 Administrator Settings

1. In the tab `Administrator settings` we can define the email address that will receive email alerts about Firewall activities.
2. **Centrora Google Authenticator**. This function is to unblock the administrator IP if it's falsely blocked. After enabling it, please scan the barcode with the Google Authentication App on our mobile. Also, there will be a field on the front-end ban page.

Whenever your admin IP is blocked out, you can access the Google Authentication App on your mobile to get the code. After submitting the code there, your IP will be immediately whitelisted and you will get the website access back.

11.4 Ban Page SEO

Edit SEO to make the Firewall SEO friendly in case the search engine indexing/crawling is filtered/blocked/affected. For example, if a Google crawler is blocked, it might not detect website data and show website information in the search result correctly. In this case, the Firewall will send SEO information that you have set here to Google. However, please note that this is only a temporary solution and the best way is to find out the reason of the false blocks and to whitelist the related rules or variables which cause the false alarms.

If parameter is set as OFF for search engine (Google, Yahoo, and MSN) bots, the Firewall will bypass all visits from the specific search engine, hence there will be no false blocks for that search engine. Nevertheless, it is worth noting that there is a small potential risk here. Our past experience has observed that some hackers can disguise their IPs and activities to make them look like from Google bots. Bypassing Google bots will allow the access of this kinds of hackers.

11.5 Country Blocking

This function allows you to block IPs from the specific countries. Please note that you need to download Country Database under the menu `Firewall Settings --> Country Blocking` before the function can be used.

After downloading the data, the full list of countries will be shown. You can choose a country and use the Blacklist Country to block visits from a specific country.

11.6 Brute Force Protection

With the function enabled, a user's account will be blocked when the maximum number of login attempts is reached within a given time period.

11.7 Google 2-Step Verification

2-Step Google Authentication is only available for the WordPress and Joomla! currently. This function guarantees login security of a much higher level. Before the settings, you will need to install the Google Authenticator App on your mobile.

First, enable **Google 2-Step Verification** in the tab `Brute Force Protection`.

Then for Joomla!, please go to the menu `Users --> Manage`, edit the profile for the admin user in the tab `Two Factor Authentication`. Set Authentication Method as **Google Authenticator** and follow the steps there to finalize the setup.

For WordPress, please go to the menu `Users` and edit the admin account. In the section **Google Authenticator Settings**, set it Active. Click **Show/Hide QR code** to have the barcode showing and scan it with the mobile. Save the settings.

After this is set, the google authenticator app from your smart phone will generate a code every minute, which makes your login highly secure. Even if a hacker knows your username and password, he will not able to access the site administrator area without the google authenticator code.

11.8 Load Firewall Rules

After the setting is done, please double check the firewall rules are loaded. Please go to menu `Firewall Settings --> Firewall Rules Fine-tuning`. In `Advanced Firewall Rules`, there is a button showing Firewall Update allowing you to do a manual update, if you have subscribed to our premium service. Thereafter, the Rules will be automatically updated.

The configuration is all done. Your sites are now under protection by the firewall system.

CHAPTER 12

Test Firewall Protection

After enabling the Firewall, we need to have a test to make sure it works to protect the website.

First, please make sure the Firewall is enabled and the setting is saved.

We can test the Centrora Firewall function using the URL:

```
http://your_site_URL/index.php?a=%27union
```

Then you can go to the menu Firewall -> IP Management to check if your IP will be logged there. .

If the test doesn't return the expected result, please check if you have ModSecurity installed on the server if you manage the server. ModSecurity may filter the testing query first. If not the case, it means the protection is not enabled well. Please contact us at our Support Center for help.

CHAPTER 13

Manage IPs and Variables

After the firewall is turned On, the IP records will be logged in the menu `Logs --> Web Attacks`.

13.1 IP Status

An IP record can have 3 states, **Whitelisted**, **Blacklisted**, and **Monitored**.

- **Whitelisted** (marked as a green check) means the IP will not be scanned by the Firewall core engine;
- **Blacklisted** (marked as a red stop symbol) means the IP will be thoroughly blocked from the site and receive the block message;
- **Monitored** (marked as a yellow eye) means the IP is only logged in IP Management for the admin attention and the IP will still have access to the site.

13.2 Manage IPs

We can also manage the IPs in the same menu with the functional buttons.

- **Add IP**: It can add new IP rule to define new IP or IP range whitelist and blacklist. In the IP RuleTitle field, you can input anything which can remind you of the reason for adding the rule.
- **Blacklist IPs/Whitelist IPs/Monitor IPs**: You can use these buttons to switch between different IP states for a chosen IP.
- **Delete Items/Clear All Items**: To delete some or all existing IP rules in the IP Management.
- **Update Host**: To keep the host information of the IP up to date.
- **Import/Export IP from/to CSV**: The tool for importing or exporting IP rules.

13.3 Check IP Record Details and Whitelist

Generally we need to check the IP record details to find the reason for being logged in IP Control to judge if it's a real hacking attack or a false alert, especially when you just start using the Firewall system. Based on the detailed information, you can whitelist the false alerted variables to make the system fit your site's functions and make it more stable. To do this, please click on Action following an IP to review the details first.

As the screenshot shows, you can find two important values `Detected Variable` and `Detected Content`. From the example of test with index.php?a=%27union, the variable is "get.a" and the blocked content is "union". You can know it's a hacking attack from the blocked content. If the content is some legitimate text, for example you submit some text in the article which contains a sensitive word falsely alerted, you need to set the IP as "Monitored" and also whitelist the Variable in Variables Management to avoid it happening again in the future.

13.4 Whitelist Variables

When you believe an IP is falsely logged and the variable is frequently falsely alerted, you can whitelist the variable in Variables Management. Go to the menu `Firewall Setting --> Variables Fine-tuning`. Let's still take the above test as example and assume it's a false alert. You can find all existing logged variables there and locate the one which we are going to whitelist based on the variable value "a". Choose the variable and use the "Ignore the Variable" button to whitelist it.

In the Variables Management section, each variable also has 3 possible states to choose from.

- **Scan the Variable**: It means the Firewall engine will actively scan for the variable's content and block the IP if it violates the Firewall rules.
- **Filter the Variable**: It means the Firewall engine will still scan the variable's content and log any suspicions, but it will not block the IP. This it for cases in which you are not sure whether the variable needs to be whitelisted and want to collect more information.
- **Ignore the Variable**: This means the variable is thoroughly whitelisted and the variable's content will not be scan any more.

13.5 Load Default Whitelist Variables

We strongly recommend you to load the default whitelist variables to reduce the number of false blocks for a normal website.

CHAPTER 14

File Upload Validation

Centrora Security integrates a File Upload Validation function to stop the malware files upload from the website forms.

Note: Please note that the *FILEINFO* module needs to be installed properly on the server to have the function working correctly. More information about *FILEINFO* can ne found at: http://php.net/manual/en/ref.fileinfo.php

14.1 Switch On/Off File Upload Validation

If there is no *FILEINFO* on the server or if you have any trouble uploading files even with the extensions whitelisted, please disable the function in the menu `Firewall Setting --> Firewall Rules Fine-tunings --> Basic Firewall Rules`, page 2, **File Upload Validation** by clicking the Status icon to make it inactive.

14.2 Configuration

First, the feature will only allow the files to be uploaded with extensions that you mark as **Allowed**. Also, it will scan the extension of the uploaded files to check the consistency of its extension and the real type. This will block the files with hacking codes embedded. Please configure the settings in the menu “”Logs –> File Uploading Logs –> FIle Extension List‘‘. The extensions with a green check are allowed to make uploads while those with a red cross are not. You can also add more extensions if the default list doesn’t include your file type.

In the tab of the same menu `File Uploading Log`, you can check all the files uploaded/blocked with the function enabled. When the site has any anomaly, you might need to investigate all the changes made to the site within a certain period of time, and this can be helped by the log.

CHAPTER 15

Configure Firewall Settings of Centrora Version 7

15.1 Basic Firewall Settings

To enable the firewall and configure the basic settings, following the Wizard is recommend as is an easy way to go through all major settings, especially for new users. We suggest you to enable all parameters for the best protection.

After the setting is finished, the main panel will show the overall status of the firewall protection, where you can further adjust the settings based on your own needs.

15.2 Firewall Protection Mode

There are three modes when the firewall detects suspicious activities.

15.2.1 1. Blocking Mode [Premium User]

Blocking mode uses the combination of attempt count and firewall sensitivity to determine whether to block a user or not. By default, the attempt counts are set to 10 and the firewall sensitivity is set to level "sensitive". In this case, when the front-end visitors trigger over 10 times of operations/queries which are detected by the firewall at the "sensitive" standard, the visitors' IPs will be blocked. To make the firewall stricter towards attackers, you can lower down the attempt count and increase the firewall sensitivity. Once the user is blocked, he/she will not be able to view the website and will only see the ban page.

This mode is recommended for users who want to keep a strict security standard and do not want any suspicions to access the website.

15.2.2 2. Filter Mode [Premium User]

Filter mode works differently from Blocking mode and in a more friendly way for front-end users. This mode focuses more on filtering and cleaning malicious requests/queries instead of blocking the IPs thoroughly. Under this mode, all

suspicious activities will be silently filter and are not able to enter the website, meanwhile, it will not block the user IPs to avoid the confusion for users who make false positives.

However, it is important to note that this mode will still block users who perform attacks including,

1. Spamming
2. Using malicious user agents
3. Malicious file uploads
4. Brute force

15.2.3 3. Logging Mode [Free User]

Logging mode is specially applied for free users. In this mode, the system will only keep track of attacks and will not block the attacker nor filter the request. The attack information can be viewed in the IP management page. The logging mode will send the alert email to the administrator when an attack is detected, and manual actions are required to block the IPs that trigger attacks. If the website is frequently attacked, it's recommend to subscribe our premium service to have the above 2 mode available to automatically block attacks.

15.3 Brute Force Protection

Note: Brute Force protection needs to work with website system plugin to detect the user login, so it's not available for Centrora Security Suite. We will try to add this feature in the future version of Centrora Suite.

Brute Force will detect the failure times of user login. With the function enabled, a user's account will be blocked when the maximum number of login attempts is reached within a given time period.

Also, a two-step Google authentication can be setup in order to make the website back-end immune to brute force attacks. Please follow the steps below to set it up.

15.3.1 For Joomla

1. Click on the `ON` button to switch it active in the Brute Force section -> Google Verification tab.
2. A pop-up message will be shown for the confirmation. Click to continue.
3. You will be automatically redirected to the user's profile page in Joomla User Management.
4. Go on User Profile, enter the Two factor authentication tab and choose **Google Authenticator** as the authentication mode.
5. You will need to scan the barcode using the Google Authenticator app on your mobile phone. After scanning the barcode, the app will generate a 6-digit code.
6. Return to Joomla! User Profile and fill this code in the step 3 of the same page.
7. Once the code is validated, the setup is completed. The google authenticator app from your smart phone will generate a code every minute when you need to login, which makes your login highly secure. Even if a hacker knows your username and password, he will not able to access the site administration area without the google authenticator.
8. **Now, it's very important to go back to the previous Centrora Panel page to SAVE the configuration.**
9. Please set the 2-step authentication for all admin accounts.

15.3.2 For WordPress

1. The same, click on the `ON` slider to enable in the Brute Force section -> Google Verification tab.
2. A pop-up message will be shown for the confirmation. Click to continue.
3. You will be redirected to the user's profile page in the WordPress User Panel.
4. Tick the "Active" box and scan the barcode using the Google Authenticator app on your mobile phone. After scanning the barcode, the app will generate a 6-digit code. Save the setting.
5. After this is set, the google authenticator app from your smart phone will generate a code every minute when you need to login, which makes your login highly secure. Even if a hacker knows your username and password, he will not able to access the site administration area without the google authenticator.

15.4 Ban Page SEO

Edit SEO in the menu `Advance Settings` –> `SEO Configuration` to make the Firewall SEO friendly in case the search engine indexing/crawling is filtered/blocked/affected. For example, if a Google crawler is blocked, it might not detect website data and show website information in the search result correctly. In this case, the Firewall will send SEO information that you have set here to Google. However, please note that this is only a temporary solution and the best way is to find out the reason of the false blocks and to whitelist the related rules or variables which cause the false alarms.

If parameter is set as OFF for search engine (Google, Yahoo, and MSN) bots, the Firewall will bypass all visits from the specific search engine, hence there will be no false blocks for that search engine. Nevertheless, it is worth noting that there is a small potential risk here. Our past experience has observed that some hackers can disguise their IPs and activities to make them look like from Google bots. Bypassing Google bots will allow the access of this kinds of hackers.

15.5 Country Blocking

This function allows you to block IPs from the specific countries. Please note that you need to download Country Database under the menu `Advance Settings` –> `Country Blocking` before the function can be used.

After downloading the data, the full list of countries will be shown. You can choose a country and make the shield icon to **Red** to block visits from a specific country. Moreover, if you set the shield as **green**, the country will not be scanned by the firewall and all IPs from the country can access the website without any monitor. A **yellow** means the country will be under the firewall's monitor normally.

CHAPTER 16

Manage IPs and Variables

From Centrora Version 7, the IP records and Logs can be easily found in the menu `IP Management` from the Firewall V7 main panel.

16.1 IP Status

An IP record can have 3 states, **Whitelisted**, **Blacklisted**, and **Monitored**.

- **Whitelisted** (marked as a green check) means the IP will not be scanned by the Firewall core engine;
- **Blacklisted** (marked as a red stop symbol) means the IP will be thoroughly blocked from the site and the users from the IP will receive the block message on the site front-end;
- **Monitored** (marked as a yellow eye) means the IP is only logged in IP Management for the admin attention and the IP will still have access to the site.

16.2 Manage IPs

We can also manage the IPs in the same menu with the functional buttons.

- **Add IP**: It can add new IP rule to define new IP or IP range whitelist and blacklist. In the IP Rule Title field, you can input anything which can remind you of the reason for adding the rule.
- **Blacklist IPs/Whitelist IPs/Monitor IPs**: You can use these buttons to switch between different IP states for a chosen IP.
- **Delete Items/Clear All Items**: To delete some or all existing IP rules in the IP Management.
- **Import/Export IP from/to CSV**: The tool for importing or exporting IP rules.
- **Temporarily Whitelist IPs**: It's a new feature from Firewall version 7. While adding a whitelist IP, you can define how long time the IP will be whitelisted. With the button `Get Temp Whitelisted IPs`, you can manage the temporarily whitelisted IPs. It's very useful when you want to grant the website access without

any firewall monitor to specific users for a time period. For example when you have developers working on the website to update codes or add new contents, you can use the function to whitelist them during they are working.

16.3 Check IP Record Details and Whitelist

Generally, whenever an IP is logged, we need to check the IP record details to find the reason to judge if it's a real hacking attack or a false alert, especially when you just start using the Firewall system. Based on the detailed information, you can whitelist the false alerted variables to make the system better fit your website's functions. Please click on Action following an IP to review the details first.

As the screenshot shows, you can find two important values `Detected Variable` and `Malicious Pattern`. From the example of test on the image, the variable is "get.abc" and the pattern is "123456../../../.....". You can know it's a hacking attack from the pattern. If you believe the content is some legitimate text, for example you submit some text in the article which contains a sensitive word falsely alerted, you need to set the IP as "Monitored" and also whitelist the Variable in Centrora Firewall Panel –> Advance Settings –> Variables Management to avoid it happening again in the future.

16.4 Whitelist Variables

When you believe an IP is falsely logged and the variable is frequently falsely alerted, you can whitelist the variable in Variables Management. Go to the menu `Centrora Firewall Main Panel --> Advance Settings --> Variables Management`. Let's still take the above test as example and assume it's a false alert. You can find all existing logged variables there and locate the one which we are going to whitelist based on the variable value "abc". Choose the variable and use the "Ignore the Variable" button to whitelist it.

In the Variables Management section, each variable also has 3 possible states to choose from.

- **Scan the Variable**: It means the Firewall engine will actively scan for the variable's content and block the IP if it violates the Firewall rules.
- **Filter the Variable**: It means the Firewall engine will still scan the variable's content and log any suspicions, but it will not block the IP. This it for cases in which you are not sure whether the variable needs to be whitelisted and want to collect more information.
- **Ignore the Variable**: This means the variable is thoroughly whitelisted and the variable's content will not be scan any more.

16.5 Load Default Whitelist Variables

We strongly recommend you to load the default whitelist variables to reduce the number of false blocks for a normal website.

CHAPTER 17

File Upload Validation

Centrora Security integrates a File Upload Validation function to stop the malware files upload from the website forms.

Note: Please note that the *FILEINFO* module needs to be installed properly on the server to have the function working correctly. More information about *FILEINFO* can ne found at: http://php.net/manual/en/ref.fileinfo.php

17.1 Switch On/Off File Upload Validation

If there is no *FILEINFO* on the server or if you have any trouble uploading files even with the extensions whitelisted, please disable the function in the menu `Firewall Main Panel --> File Upload Control`.

17.2 Configuration

First, the feature will only allow the files to be uploaded with extensions that you mark as **Allowed**. Also, it will scan the extension of the uploaded files to check the consistency of its extension and the real type. This will block the files with hacking codes embedded. Please configure the settings in the menu `Advance Settings --> File Extension Control Table`. The extensions with a green check are allowed to make uploads while those with a red cross are not. You can also add more extensions if the default list doesn't include your file type.

In the menu `File Upload Logs`, you can check all the files uploaded/blocked with the function enabled. When the site has any anomaly, you might need to investigate all the changes made to the site within a certain period of time, and this can be helped by the log.

CHAPTER 18

Centrora Security Basic Firewall Rules Explanation

- Enable Stop Forum Spam Scanning

This will check if the IP address being scanned or the email address being scanned has been marked as spammers from the Stop Forum Spam website.

- Block Blacklisted Methods (Trace / Delete / Track)

Every time a client attempts to connect to your server, it sends a message indicating the type of connection it wishes to make. There are many different types of request methods recognized by Apache. The two most common methods are `GET` and `POST` requests, which are required for "getting" and "posting" data to and from the server. In most cases, these are the only request methods required to operate a dynamic website. Allowing more request methods than are necessary increases your site's vulnerability. Here we are blocking delete and head because they are unnecessary, and also blocking trace and track because they violate the same-origin rules for clients. (Reference: Perishable Press)

- Checks Malicious User Agent

Blocking hundreds of the worst bots can ensure open-access for normal traffic, major search engines (Google, Bing, et al), good browsers (Chrome, Firefox, Opera, et al), and everyone else. Blocking malicious user agent can help you avoid traffics that are known to be associated with malicious activity

- Checks Cross Site Scripting (XSS)

XSS attacks occur when an attacker uses a web application to send malicious codes in order to access cookies, session tokens or other sensitive information retained by the browser and used with the website, and rewrite contents of the html page.

- Checks Cross Site Request Forgery (CSRF)

CSRF is an attack that forces end users to execute unwanted actions in a web application in which they are currently authenticated. It could make end users perform state changing requests like transferring funds, changing email addresses, or even compromising the entire web application.

- Checks Basic DoS Attacks

This helps prevent your website against the HTTP Flood Attacks at the web application level. Massive crawling / scanning tools, HTTP Flood tools can be detected and blocked if it exceeds the defined thresholds / number of visits to your website in a specific time.

- Checks Basic Remote File Inclusion

Remote File Inclusion (RFI) is a type of vulnerability most often found on websites. It allows an attacker to include a remote file, usually through a script on the web server. The vulnerability occurs due to the use of user-supplied input without proper validation.

- Checks Basic Direct File Inclusion

Direct File Inclusion / Local File Inclusion (LFI) is similar to a Remote File Inclusion vulnerability except instead of including remote files, only local files i.e. files on the current server can be included. The vulnerability is also due to the use of user-supplied input without proper validation. (Reference: WikiPedia)

- Checks Format String Attacks

The Format String exploit occurs when the submitted data of an input string is evaluated as a command by the application. Attackers may execute the code, read the stack, and cause a segmentation fault in the application which ultimately compromises the system.

- Checks Inconsistent File Type Upload

Uploaded files represent a significant risk to applications. Hackers can disguise the malicious codes into some common formats and upload them to the website to execute. The check on the file type will compare the real file type and the file extension in the name to filter out potential virus files.

- Checks File Codes for Virus file

It will call the file scanning function in the Dynamic Scanner to analyse the file codes. Files containing the codes violating specific virus signature/patterns will be blocked out.

- Checks Basic Javascript Injection

JavaScript injection is a nifty little technique that allows you to alter a sites contents without actually leaving the site. This can be very useful when to say, you need to spoof the server by editing some form options. This includes I. Injection Basics, II. Cookie Editing and III. Form Editing

- Checks Basic Database SQL Injection

SQL injection is a technique where malicious users can inject SQL commands into an SQL statement, via web page input. Injected SQL commands can alter SQL statement and compromise the security of a web application.

- Detect Directory Traversal

A directory traversal (or path traversal) consists in exploiting insufficient security validation / sanitization of user-supplied input file names, so that characters representing “traverse to parent directory” are passed through to the file APIs. (Reference: WikiPedia)

- Checks Brute force

With Brute Force, attackerd will be able to steal the login credentials of the website as well as the database.

CHAPTER 19

About Centrora Git backup

Choosing a proper backup way is always an important topic for website administrators. It helps keep the site data safe and guarantees that we have the latest working version under any circumstances. Super fast, efficient, and reliable, the technology with Git, which brings us many miracles, strives to provide the best solution for the object.

Why choose Git?

Git is a popular modern version control system. You can think Git as a small software which constantly monitors for the changes of the file system. Unlike the traditional backup method, which will pack all the files into an archive file, Git will only keep track of changed files. Compared to traditional backup methods, the technology with Git has 4 significant advantages.

19.1 1. Efficient in resource consumption

As mentioned above, Git only tracks the changes. So it will not keep the full website files and data upon each backup. Only changes will be committed to the last backup package and it just records the complete history. So after the first time initialization, it takes much less space and saves a lot of time in a new backup. To make a comparison, let's take an example of a website with 100MB originally and assume the size increases by 5MB every day due to new contents, user data, and logs and we make a full backup for the site every day. So the site size will be 105MB on the 2nd day, 110MB on the 3rd day, 115MB on the 4th day,and so on. At the beginning, the backup package size is 100MB, the same for the traditional and Git methods.

Day	Site Size	New Backup - Traditional Method	New Backup - Git Method
1	100 MB	100 MB	100 MB
2	105 MB	105 MB	5 MB
3	110 MB	110 MB	5 MB
4	115 MB	115 MB	5 MB
5	120 MB	120 MB	5 MB
6	125 MB	125 MB	5 MB
7	130 MB	130 MB	5 MB
8	135 MB	135 MB	5 MB
9	140 MB	140 MB	5 MB
10	145 MB	145 MB	5 MB
Accumulation		*1225 MB*	*145 MB*

However, we can observe the dramatic difference just after 10 days. With the traditional method, it keeps the full daily backups. So if we save the backup packs for all the 10 days, the total space on the server reaches 1225 MB; while the Git method only consumes 145MB as it only commits the change of 5MB every day, at the same time, the backup time being largely shortened as well.

19.2 2. Super fast in rollback

With the traditional method, if our website gets hacked, we must do a full restoration. That means, we need to carefully go through the steps including, removing all the current files, uploading or extracting the files from a previous version to the server, removing the database, and restoring or importing the data from a previous backup too. Generally, it will take about 30 minutes and lots of operations. With the Git method, just one click can resolve all the issues and it could just take less than 30 seconds because it only rollback the changed contents based on the previous version.

19.3 3. Easy to track the differences

Sometimes, we need to compare the files between different versions for development or security purposes. Generally, it's a big trouble especially when the site has a large number of files, because it needs us to build a mirror, restore all files of both versions, compare the files with the MD5 Hash and even manually review the codes. With the Git functions, it will be as easy as pie. Git is designed to have a complete history and full version tracking abilities. With a few operations, we can get a full list of changed files and also the detailed changed codes of each file.

19.4 4. 10GB cloud upload with GitLab for each website

Cloud backup is a popular solution as we can easily bring the backup with we at any place at any time as long as there is an internet connection. Nowadays, all major Cloud services provide quite a large storage space and we may get more by paying extra for the service. However, it's still limited. The consideration of space will more or less restricts the freedom of keeping the backup in a long term. This is not a problem at all for Git solution. With GitLab free service, we can create unlimited repositories, Git work directories, and each repository offers 10GB space. It becomes so easy to keep the full history for a website as long as we want.

Note: If your website has very many media files it is recommended that you store them in different locations than your website directory. One of the drawbacks of using Git is it does not handle media files very well as it keeps track of every line of files. So, when it tries to manage the version of the media files it has to store a lot of information about the media files and thus the Git folder may swell up and consume too much space.

CHAPTER 20

Centrora Git Backup

Centrora Git backup provides the best ever experience on the website backup and restoration. The backup function becomes stable and efficient since Version 6.8. Some new features with Git Backup were released as well to make it easier to use and more helpful, for instance, the ability of define the custom commit title and the file changes tracking function.

Please follow the below steps to set it up and refer to the videos for how to enjoy all functions of Centrora Git backup

20.1 1. Initialize Git Backup

When you use Git Backup for the first time, it needs to initialise the database and function. If all requirement checks are fulfilled, the Dashboard of Git Backup will automatically show the button `Enable GitBackup 'Now'`. Click the button and the system will do the first backup.

After it's done, it shows the result of the first backup. The first backup will be named as "Initial Local Backup:" by default. Take a Joomla! site as the example, the backup list each core directory of the root separately to ensure the stability.

You can also check the video about how to enable Git Backup.

20.2 2. Make a New Backup

Now we can make a new backup at any time. The backup will be much faster then the initial backup because the Git technology only track and commit the changes from the initial one. Click the button `Create local backup` to make a new backup and here we can name the backup.

After it's done, the new backup will be added to the list. Please note that in the new backup,only the changed directories from the last backup are listed.

20.3 3. Track the Website Changes with Git

With the Git backup, we can easily track all changed files from the last backup. Click the ‘‘Information‘‘button following a backup to have all changed files in the specific directory listed in a pop-out window.

20.4 4. Restore the Website to a Previous Backup

Rolling back the website to a previous status is every easy, generally in seconds. Click the *Restore* button of a backup to go back to it. It will pop out a window to confirm if you would like to restore the database as well.

- Close - It will close the pop-out window and do nothing.
- No - Only restore the file system to the previous backup while keep the database unchanged.
- Yes - It will restore both the file system and database to the previous state.

20.5 5. Upload to Cloud

The backup can be uploaded to Cloud so that you can keep the backup safely even when the server gets any problem. Now Centrora Backup integrates with GitLab which provides up to 10GB space for each repository. If you have multiple websites, it can create multiple repositories under the same account. The number of repositories is unlimited. Please create an account on GitLab Website first if you don't have a GitLab account yet.

After the account is created, please to the `Settings` –> `Account` menu to get the information of **Username** and **Private Token**. These two values are used to login you account in Centrora, and also Username is very important to define the web link where you can access all your existing repositories.

Now, go back to Centrora Git Backup page and login with the above account.

If there are changes on teh website from the last backup, it will also ask you to create and name a new backup first. Then the upload will automatically start. After it completes, you can find the backup has been uploaded to your account on GitLab at: https://gitlab.com/users/**your_username**/projects.

Now the website is backed-up successfully on both local and cloud with Git. You can rescue the website with the backup easily from any emergency. If your server crashes or the website is totally down and you need a complete restoration, please refer to the guidance of ":ref: *restore-website-from-cloud*".

CHAPTER 21

Using Git Backup in Centrora Suite on WHM server

21.1 1. Pre-requisites

If it's the first time you use Git Back in Centrora Suite and the system has not been initiated, the screen will show as the screenshot when you enter Git Backup Panel.

Since centrora is installed at the server root, it needs the database access of the website in a specific account. In order to do so we need to initiate the account which will allow centrora to get the database access. Please click on the `Initiate` button next to the account and it will try to retrieve the database details within the account based on the website system, Joomla! or WordPress. Once Git has been initialized for an account, it will look like this,

Notice that after the initialization, the button next to the account name changes to `Go to the Account` which means the system is able to retrieve the database detail.

In case the system fails to retrieve the database detail it will show up a pop-out window allowing you to manually input the database info.

After setting the database connection, the system will check if the server settings satisfy the requirements of running Git. It will show the detailed report if any requirement is not fulfilled.

21.2 2. Enable the Backup

Now we can enable Git Backup if all requirement checks pass and it shows the successful window.

It will automatically start the first backup of the files and database.

Once the initialization is done, the page will redirect you to the main backup management panel which displays the list of all backups of the account.

Unlike the traditional backup method, Git backup will not show the backup history which includes a list of packages each for a whole website backup. Instead it shows a list of backups carried out over time each only tracking the changes from the previous backup.

21.3 3. Uninstall Git

This will delete all Git files and the plugin will stop tracking for all the changes. Then all your backups and the backup history will be deleted. If you have performed a cloud backup previously, it will dis-link the cloud account but the repository will still exist in the cloud account.

21.4 4. Create Local Backup

This will make a backup of the site database and the files. Once the process is completed the system will have a snapshot of the files in the system. After clicking on the `Create local backup` icon , it will show a pop up like this :

Here you can name the current backup to remark the purpose of the backup.

21.5 5. Push Backup to cloud

This feature will perform a local backup first and then upload it to your cloud account on GitLab. Please note that to use this feature, you might need to control the website size under 10GB as each repository with GitLab has a limit of 10 GB of cloud space.

Please refer to the tutorial Upload Git Backup to CLoud

21.6 6. Backup Notification

When the red dots next to the local backup and cloud backup are shown as in the previous screenshot, it basically means that the system detects new changes and suggests the admin to backup for the new changes.

21.7 7. Backup Control Panel / Accounts List for WHM Accounts

The purpose of the control panel is to provide the administration accessibility to view the status of backups of different accounts and perform backups directly without entering each account.

CHAPTER 22

Restore Website from Cloud

Centrora Git Backup with the cloud space provides a secure zone for the website backup. Even when the site is down or files are erased by the hacker, we can restore it from the cloud backup.

22.1 Download the Restore Script

Please download the restore from Cloud script here.

22.2 Instruction

1- Upload the script package to the directory where you would like to restore the website from the GitLab backup, say /httpdocs/test/.

2- Run the script as:

```
http://your_site_URL/test/git.php
```

3- It will show a very simple panel where you can input the GitLab backup package information.

4- On the form, the Git URL can be found from your GitLab account. Go to the Personal projects menu in GitLab after login and go to the project which you want to restore.

On the project page, choose **HTTPS** and copy the link.

5- Then go back to the Git restore page. Fill the form and click *Restore from Git*. It will show the brief download progress. The download is complete when it shows **The git has been pulled successfully**. It will redirect to the database restoration page automatically.

6- Now check the target directory /test, and we can find all files have been there.

7- Next, we need to prepare a database (better to be an empty one) and manually enter the Database information into above “Restore Database” page. Then *Restore database*.

The restoration is done.

CHAPTER 23

Scheduled Tasks

Centrora Security allows you to setup various scheduled tasks. It simplifies the configurations so you don't have to set cron jobs in the host control panel.

We can create the tasks in the menu `Scheduled Tasks`.

For the **Scheduled Virus Scanning**, it can be defined as frequent as daily. However, if the website is clean, making it daily is not that necessary. We will recommend to set the scheduled scan as every week.

For the **Scheduled Git Backup**, we recommend setting it to run every 24 hours.

CHAPTER 24

Email Settings

24.1 Receive Email Notifications

To receive the email notifications for the events on the website, such as Firewall block alerts and Scheduled scan report, please simply enter your email address in the menu `Firewall Settings` –> `Firewall Configuration` –> `Administrator Setting`.

If you would like to receive Centrora Update Notification, please tick the option **Receive Update Email** as well.

24.2 Customize Email Template

The Firewall alert email can be customized based on your needs. Please go to the menu `Management` –> `Manage Administrators` and click `Edit Email` to edit the email template.

Note: You can edit the template, such as the images. color, font, etc. but please don't change the contents with the braces because they are the variables from which the system gets the information.

CHAPTER 25

Fatal error: Class PDO

Error: Class PDO not found

If you encounter the error `Fatal error: Class 'PDO' not found` when the OSE Firewall is activated, this indicates the Class 'PHP Data Objects' is not loaded in your PHP environment. You can do a check to confirm if the class exists.

1 Make a new php file in your site root directory with name `check_pdo.php`.

2 Put the below codes into the file:

```
<?php
  if (extension_loaded('pdo')) {
  echo "PDO is installed.";
  } else {
  echo "PDO is NOT installed.";
  }
?>
```

3 Run the script on the site through the URL: *http://your_site_domain/check_pdo.php* and it will show the PDO status.

PDO is activated by default as of PHP 5.1.0, so if it's disabled please contact your hosting company to enable it.

Reference: http://www.php.net/manual/en/pdo.installation.php

If you manage the server or know how to customize the PHP configurations, please edit the php.ini file to add the following codes into it:

```
extension = pdo.so
extension = pdo_mysql.so
```

Once PDO is added to the PHP environment, issue will be resolved.

Error: Connection failed:SQLSTATE[HY000] [2002] No such file or directory. Fatal error: Call to amember function prepare() on a non-object

If you encounter this error, it means the PDO MySQLsocket might be missing on your server. Please upload an `info.php` file to the server with the codes:

```
<?php
  phpinfo();
?>
```

Run the script through: *http://your_site_domain/info.php* to check the server PHP settings.

Search for `mysql.default_socket`,and you could find its value is `/var/run/mysqld/mysqld.sock`.

Then search for `pdo_mysql.default_socket`. It always returns a different value, for example `/tmp/mysql.sock`. This is where the problem is. This directory might be missing or un-writable. The solution is to edit your server PHP settings to define:

```
pdo_mysql.default_socket = /var/run/mysqld/mysqld.sock
```

Or please contact your host for the help if you are not allowed to change PHP settings on the server.

CHAPTER 26

Joomla Fabrik Component Conflict

If you are using the Joomla! Fabrik Component and encounter the following error in the browser console,

```
Error: Mismatched anonymous define() module: function init($, undefined) {     ....
↪require.js
```

This indicates the Fabrik Component System plugin is causing the conflicts with Centrora Security.

To resolve this, please open this file,

```
/plugins/system/fabrik/fabrik.php
```

Find the following lines,

```
public function onAfterRender()
{
// Could be component was unistalled but not the plugin
if (!class_exists('FabrikString'))
{
return;
}
```

Add the following codes to the plugin file,

```
$option=JRequest::getVar("option","");
if ($option =='com_ose_firewall')
{ return; }
```

This will sort out the issue.

CHAPTER 27

Signature Update Failure

If you come across Error of update database failure when updating the Signature or the Virus patterns, please check the below paths and set the permission of the folders into "777".

For CentroraJoomla! version or Centrora Suite,

```
/administrator/components/com_ose_firewall/protected/data
/administrator/components/com_ose_firewall/protected/data/tmp
/administrator/components/com_ose_firewall/protected/data/vsscanpath
```

For WordPress version,

```
/wp-content/plugins/ose_firewall/protected/data
/wp-content/plugins/ose_firewall/protected/data/tmp
/wp-content/plugins/ose_firewall/protected/data/vsscanpath
```

If the Virus Signature date in Dynamic Scanner stays as an old date, please try to remove the file:

For Joomla!,

```
/wp-content/plugins/ose-firewall/protected/data/tmpLastVersionCheck.php
```

For WP,

```
/administrator/components/com_ose_firewall/protected/data/tmpLastVersionCheck.php
```

Then go back to the Dynamic Scanner and refresh page. The updater should reload again.

CHAPTER 28

Whitelist Variables

If the IP or activity is falsely blocked, please follow the steps to whitelist the variables/rules:

1. Go to Centrora menu `IP Management` to locate the IP.
2. Check the details by the `Information` button for the value of **Detected Variables**.
3. Go to the menu `Advance Settings -> Variables Management`, find the variables above and whitelist them.
4. Go back to the `IP Management` menu to remove your logged IP.

Or please refer to *Check IP Record Details and Whitelist* for more details.

CHAPTER 29

List of Video Tutorials