Webseiten-Bericht für seguridadwordpress.es

Generiert am 19 Mai 2025 20:39 PM

Der Wert ist 54/100

SEO Inhalte

✓	Seitentitel	SeguridadWordPress.es - Recopilación de vulnerabilidades WordPress. Länge : 67 Perfekt, denn Ihr Seitentitel enthält zwischen 10 und 70 Anzahl Zeichen.
⚠	Seitenbeschreibung	Recopilación de vulnerabilidades WordPress. Länge : 43 Ideal, aber Ihre Seitenbeschreibung sollte zwischen 70 und 160 Zeichen (Leerzeichen incinbegriffen) enthalten. Benutzen Sie dieses kostenlose Werkzeug um die Länge zu prüfen.
✗	Suchbegriffe	Nicht so gut. Wir konnten keine META-Suchbegriffe auf Ihrer Webseite finden. Benutzen Sie dieses kostenlose Werkzeug um META-Suchbegriffe zu erzeugen.
✓	Og META Eigenschaften	Sehr gut, denn diese Webseite nutzt die Vorteile aus den Og Properties.

Eigenschaft	Inhalt
locale	en_US
type	website
title	SeguridadWordPress.es
description	Recopilación de vulnerabilidades WordPress.
url	https://seguridadwordpress.es/
site_name	SeguridadWordPress.es

●	Überschriften	H1 0	H2 11	H3 1	H4 0	H5 0	H6 0

- [H2] Ultimas Noticias

SEO Inhalte

		• [H2] WP All Import Pro <= 4.9.7 – Cross-Site Scripting a través de la carga de archivos SVG con autenticación (Administrador+) • [H2] Vulnerabilidad de Inyección SQL en el Plugin The Ultimate WordPress Toolkit – WP Extended <= 3.0.12 a través del Módulo de Intentos de Inicio de Sesión • [H2] Vulnerabilidad CVE-2024-13385 en plugin JSM Screenshot Machine Shortcode <= 2.3.0 – XSS almacenado autenticado (Contribuidor+) • [H2] Vulnerabilidad de Cross-Site Scripting en el plugin MicroPayments – Fans Paysite para WordPress • [H2] Adifier System <= 3.1.7 – Restablecimiento de contraseña arbitrario no autenticado • [H2] Vulnerabilidad de Cross-Site Scripting almacenado en Video Share VOD – Turnkey Video Site Builder Script <= 2.6.31 • [H2] Vulnerabilidad CSRF en ShipWorks Connector for Woocommerce <= 5.2.5 • [H2] Ultimas Vulnerabilidades • [H2] Ordenados por CVE • [H2] Acerca de seguridadwordpress.es • [H3] Recopilación de vulnerabilidades WordPress.
	Bilder	Es konnten 1 Bilder auf dieser Webseite gefunden werden. Bei 1 Bilder(n) fehlt ein ALT-Attribut. Fügen Sie ALT-Attribute zu Ihren Bildern, um die Bedeutung der Bilder für Suchmaschinen zugänglich zu machen.
	Text/HTML Verhältnis	Anteil : 8% Das Text zu HTML Code Verhältnis dieser Webseite ist niedriger als 15 Prozent, was bedeutet, dass Sie mehr Inhalte für Ihre Webseite schreiben sollten.
	Flash	Perfekt, denn es wurde kein Flash auf Ihrer Webseite gefunden.
	IFrame	Großartig, denn Sie verwenden keine IFrames auf Ihrer Webseite.

SEO Links

	URL Rewrite	Gut. Ihre Links sind für Suchmaschinen gut lesbar (sprechende Links)!
	Underscores in the URLs	Wir haben Unterstriche in Ihren Links entdeckt. Benutzen Sie zur Optimierung besser Bindestriche in Ihren Links.
	In-page links	We found a total of 64 links including 0 link(s) to files

SEO Links

	Statistics	Externe Links : noFollow 0% Externe Links : natürliche Links 0% Interne Links 100%

In-page links

Anker	Typ	Natürlich
SeguridadWordPress.es	intern	natürliche Links
WP All Import Pro <= 4.9.7 – Cross-Site Scripting a través de la carga de archivos SVG con autenticación (Administrador+)	intern	natürliche Links
Vulnerabilidad de Inyección SQL en el Plugin The Ultimate WordPress Toolkit – WP Extended <= 3.0.12 a través del Módulo de Intentos de Inicio de Sesión	intern	natürliche Links
Vulnerabilidad CVE-2024-13385 en plugin JSM Screenshot Machine Shortcode <= 2.3.0 – XSS almacenado autenticado (Contribuidor+)	intern	natürliche Links
Vulnerabilidad de Cross-Site Scripting en el plugin MicroPayments – Fans Paysite para WordPress	intern	natürliche Links
Adifier System <= 3.1.7 – Restablecimiento de contraseña arbitrario no autenticado	intern	natürliche Links
Vulnerabilidad de Cross-Site Scripting almacenado en Video Share VOD – Turnkey Video Site Builder Script <= 2.6.31	intern	natürliche Links
Vulnerabilidad CSRF en ShipWorks Connector for Woocommerce <= 5.2.5	intern	natürliche Links
2	intern	natürliche Links
3	intern	natürliche Links
481	intern	natürliche Links
Rate Star Review Vote – AJAX Reviews, Votes, Star Ratings <= 1.6.3 – Cross-Site Scripting	intern	natürliche Links
Webcamconsult <= 1.5.0 – Cross-Site Request Forgery to Stored Cross-Site Scripting	intern	natürliche Links
Vulnerabilidad de XSS almacenado en Utilities for MTG <= 1.4.1 – Autenticado (Colaborador+) Stored Cross-Site Scripting	intern	natürliche Links

In-page links

MarketKing — Ultimate WooCommerce Multivendor Marketplace Solution <= 1.9.80 – Cross-Site Scripting con Autenticación (Shop Manager+)	intern	natürliche Links
Tema de WordPress Buzz Club – Night Club, DJ and Music Festival Event <= 2.0.4 – Falta de Autorización para Actualización de Opción Arbitraria Limitada a Usuarios Autenticados (Suscriptores+)	intern	natürliche Links
WP Abstracts <= 2.7.2 – CSRF a XSS Reflejado	intern	natürliche Links
Galería de Imágenes – Subidas de Imágenes en Frontend, Lista de Fotos AJAX <= 1.5.22 – Cross-Site Scripting Almacenado Autenticado (Contributor+) a través del shortcode videowhisper_picture_upload_guest	intern	natürliche Links
Jet Engine <= 3.6.2 – Cross-Site Scripting almacenado autenticado (Contributor+) a través del parámetro list_tag	intern	natürliche Links
CVE-2023-6223	intern	natürliche Links
CVE-2023-6498	intern	natürliche Links
CVE-2023-6506	intern	natürliche Links
CVE-2023-6520	intern	natürliche Links
CVE-2023-6524	intern	natürliche Links
CVE-2023-6567	intern	natürliche Links
CVE-2023-6600	intern	natürliche Links
CVE-2023-6629	intern	natürliche Links
CVE-2023-6699	intern	natürliche Links
CVE-2023-6733	intern	natürliche Links
CVE-2023-6738	intern	natürliche Links
CVE-2023-6747	intern	natürliche Links
CVE-2023-6776	intern	natürliche Links
CVE-2023-6828	intern	natürliche Links
CVE-2023-6883	intern	natürliche Links
CVE-2023-6980	intern	natürliche Links
CVE-2023-6981	intern	natürliche Links
CVE-2023-6984	intern	natürliche Links

In-page links

CVE-2023-7027	intern	natürliche Links
CVE-2023-7068	intern	natürliche Links
CVE-2023-51410	intern	natürliche Links
CVE-2023-51418	intern	natürliche Links
CVE-2023-51678	intern	natürliche Links
CVE-2023-52177	intern	natürliche Links
CVE-2024-0201	intern	natürliche Links
CVE-2024-0616	intern	natürliche Links
CVE-2024-5226	intern	natürliche Links
CVE-2024-5260	intern	natürliche Links
CVE-2024-5545	intern	natürliche Links
CVE-2024-5668	intern	natürliche Links
CVE-2024-6568	intern	natürliche Links
CVE-2024-6709	intern	natürliche Links
CVE-2024-6770	intern	natürliche Links
CVE-2024-6824	intern	natürliche Links
CVE-2024-6870	intern	natürliche Links
CVE-2024-7032	intern	natürliche Links
CVE-2024-7150	intern	natürliche Links
CVE-2024-7257	intern	natürliche Links
CVE-2024-7291	intern	natürliche Links
CVE-2024-7390	intern	natürliche Links
CVE-2024-7548	intern	natürliche Links
CVE-2024-7651	intern	natürliche Links
CVE-2024-7848	intern	natürliche Links
CVE-2024-7854	intern	natürliche Links
CVE-2024-43343	intern	natürliche Links

SEO Suchbegriffe

	Suchbegriffswolke	january cross-site wordpress plugin del almacenado para scripting través vulnerabilidad

Keywords Consistency

Suchbegriff	Inhalt	Seitentitel	Suchbegriffe	Seitenbeschreibung	Überschriften
wordpress	18	✔	✖	✔	✔
vulnerabilidad	17	✔	✖	✔	✔
cross-site	17	✖	✖	✖	✔
plugin	16	✖	✖	✖	✔
january	15	✖	✖	✖	✖

Benutzerfreundlichkeit

	URL	Domain : seguridadwordpress.es Länge : 21
✔	Favoriten Icon	Gut. Die Webseite hat ein Favicon.
✖	Druckeigenschaften	Es konnten keine druckfreundlichen CSS-Angaben gefunden werden.
✔	Sprache	Gut, denn Sie haben in den META-Elementen eine Sprache deklariert: en.
✖	Dublin Core	Diese Webseite nutzt nicht die Vorteile der Dublin Core Elemente.

Dokument

✔	Doctype	HTML 5

Dokument

✓	Verschlüsselung	Perfekt, denn Ihre Webseite deklariert einen Zeichensatz: UTF-8.
✗	W3C Validität	Fehler : 0 Warnungen : 0
✓	E-Mail Datenschutz	Sehr gut, denn es wurde keine E-Mail Adresse im Klartext auf Ihrer Webseite gefunden.
✓	Veraltetes HTML	Sehr gut! Sie verwenden aktuelle HTML Tags in Ihrem Webseitenquelltext.
●	Tipps zur Webseitengeschwindigkeit	✓ Sehr gut, denn Ihre Webseite benutzt keine verschachtelten Tabellen. ✗ Schlecht, denn es wurden CSS-Angaben in HTML-Elementen entdeckt. Diese Angaben sollten in ein entsprechendes CSS-Stylesheet verlagert werden. ✗ Nicht so gut, denn Ihre Webseite enthält sehr viele CSS-Dateien (mehr als 4). ✓ Perfekt, denn Ihre Webseite enthät nur wenig Javascript-Dateien. ✗ Ihre Webseite nutzt die Vorteile von gzip nicht.

Mobile

●	Mobile Optimierung	✓ Apple Icon ✓ META Viewport Tag ✓ Flash Inhalt

Optimierung

✓	XML-Sitemap	Perfekt! Ihre Seite hat eine XML-Sitemap. http://seguridadwordpress.es/sitemap.xml
✓	Robots.txt	http://seguridadwordpress.es/robots.txt Sehr gut! Ihre Webseite enthält eine robots.txt-Datei.

Optimierung

	Analytics	Fehlt Wir haben nicht ein Analyse-Tool auf dieser Website installiert zu erkennen. Webanalyse erlaubt die Quantifizierung der Besucherinteraktionen mit Ihrer Seite. Insofern sollte zumindest ein Analysetool installiert werden. Um die Befunde abzusichern, empfiehlt sich das parallele Verwenden eines zweiten Tools.