



Avaliação do site seguridadwordpress.es

Gerado a 19 de Maio de 2025 20:39 PM

O resultado é de 54/100



Conteúdo SEO

	Título	<p>SeguridadWordPress.es - Recopilación de vulnerabilidades WordPress.</p> <p>Cumprimento : 67</p> <p>Perfeito, o Título contém entre 10 e 70 caracteres.</p>														
	Descrição	<p>Recopilación de vulnerabilidades WordPress.</p> <p>Cumprimento : 43</p> <p>Idealmente, a Descrição META deve conter entre 70 e 160 caracteres (incluindo espaços).</p>														
	Palavras-chave	<p>Mau. Não detetámos palavras-chave META na sua página.</p>														
	Propriedades Og Meta	<p>Boa! Esta página tira vantagens das propriedades Og.</p> <table border="1" data-bbox="542 1265 1481 1758"> <thead> <tr> <th>Propriedade</th> <th>Conteúdo</th> </tr> </thead> <tbody> <tr> <td>locale</td> <td>en_US</td> </tr> <tr> <td>type</td> <td>website</td> </tr> <tr> <td>title</td> <td>SeguridadWordPress.es</td> </tr> <tr> <td>description</td> <td>Recopilación de vulnerabilidades WordPress.</td> </tr> <tr> <td>url</td> <td>https://seguridadwordpress.es/</td> </tr> <tr> <td>site_name</td> <td>SeguridadWordPress.es</td> </tr> </tbody> </table>	Propriedade	Conteúdo	locale	en_US	type	website	title	SeguridadWordPress.es	description	Recopilación de vulnerabilidades WordPress.	url	https://seguridadwordpress.es/	site_name	SeguridadWordPress.es
Propriedade	Conteúdo															
locale	en_US															
type	website															
title	SeguridadWordPress.es															
description	Recopilación de vulnerabilidades WordPress.															
url	https://seguridadwordpress.es/															
site_name	SeguridadWordPress.es															
	Cabeçalhos	<table border="1" data-bbox="542 1780 1481 1859"> <thead> <tr> <th>H1</th> <th>H2</th> <th>H3</th> <th>H4</th> <th>H5</th> <th>H6</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>11</td> <td>1</td> <td>0</td> <td>0</td> <td>0</td> </tr> </tbody> </table> <ul data-bbox="614 1892 1492 2060" style="list-style-type: none"> • [H2] Ultimas Noticias • [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 	H1	H2	H3	H4	H5	H6	0	11	1	0	0	0		
H1	H2	H3	H4	H5	H6											
0	11	1	0	0	0											

Conteúdo SEO

		<p>WordPress Toolkit - WP Extended <= 3.0.12 a través del Módulo de Intentos de Inicio de Sesión</p> <ul style="list-style-type: none">• [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] Últimas Vulnerabilidades• [H2] Ordenados por CVE• [H2] Acerca de seguridadwordpress.es• [H3] Recopilación de vulnerabilidades WordPress.
	Imagens	<p>Encontrámos 1 imagens nesta página.</p> <p>1 atributos ALT estão vazios ou em falta. É recomendado adicionar texto alternativo de modo a que os motores de busca identifiquem melhor o conteúdo das suas imagens.</p>
	Rácio Texto/HTML	<p>Rácio : 8%</p> <p>O rácio de texto para código HTML desta página é menor que 15 por cento, o que significa que provavelmente é necessário de adicionar mais conteúdos em forma de texto.</p>
	Flash	<p>Perfeito, não foi encontrado conteúdo Flash nesta página.</p>
	Iframe	<p>Excelente, não foram detetadas Iframes nesta página.</p>

Ligações SEO

	Reescrita de URL	<p>Perfeito. As ligações aparentam ser limpas!</p>
	Underscores (traços inferiores) nas URLs	<p>Detetámos 'underscores' (traços inferiores) nas suas URLs. O uso hífen é mais eficiente em termos de otimização SEO.</p>
	Ligações para a própria página	<p>Encontrámos um total de 64 ligações incluindo 0 ligações a ficheiros</p>
	Statistics	<p>Ligações externas : noFollow 0%</p> <p>Ligações externas : Passa sumo 0%</p>

Ligações SEO

Ligações internas 100%

Ligações para a própria página

Âncoras	Tipo	Sumo
SeguridadWordPress.es	Internas	Passa sumo
WP All Import Pro &lt;= 4.9.7 &#8211; Cross-Site Scripting a través de la carga de archivos SVG con autenticación (Administrador+)	Internas	Passa sumo
Vulnerabilidad de Inyección SQL en el Plugin The Ultimate WordPress Toolkit &#8211; WP Extended &lt;= 3.0.12 a través del Módulo de Intentos de Inicio de Sesión	Internas	Passa sumo
Vulnerabilidad CVE-2024-13385 en plugin JSM Screenshot Machine Shortcode &lt;= 2.3.0 &#8211; XSS almacenado autenticado (Contribuidor+)	Internas	Passa sumo
Vulnerabilidad de Cross-Site Scripting en el plugin MicroPayments &#8211; Fans Paysite para WordPress	Internas	Passa sumo
Adifier System &lt;= 3.1.7 &#8211; Restablecimiento de contraseña arbitrario no autenticado	Internas	Passa sumo
Vulnerabilidad de Cross-Site Scripting almacenado en Video Share VOD &#8211; Turnkey Video Site Builder Script &lt;= 2.6.31	Internas	Passa sumo
Vulnerabilidad CSRF en ShipWorks Connector for Woocommerce &lt;= 5.2.5	Internas	Passa sumo
2	Internas	Passa sumo
3	Internas	Passa sumo
481	Internas	Passa sumo
Rate Star Review Vote - AJAX Reviews, Votes, Star Ratings &lt;= 1.6.3 &#8211; Cross-Site Scripting	Internas	Passa sumo
Webcamconsult &lt;= 1.5.0 &#8211; Cross-Site Request Forgery to Stored Cross-Site Scripting	Internas	Passa sumo
Vulnerabilidad de XSS almacenado en Utilities for MTG &lt;= 1.4.1 &#8211; Autenticado (Colaborador+) Stored Cross-Site Scripting	Internas	Passa sumo
MarketKing — Ultimate WooCommerce Multivendor Marketplace Solution &lt;= 1.9.80 &#8211; Cross-Site Scripting con Autenticación (Shop Manager+)	Internas	Passa sumo

Ligações para a própria página

Tema de WordPress Buzz Club - Night Club, DJ and Music Festival Event &lt;= 2.0.4 &#8211; Falta de Autorización para Actualización de Opción Arbitraria Limitada a Usuarios Autenticados (Suscriptores+)	Internas	Passa sumo
WP Abstracts &lt;= 2.7.2 &#8211; CSRF a XSS Reflejado	Internas	Passa sumo
Galería de Imágenes &#8211; Subidas de Imágenes en Frontend, Lista de Fotos AJAX &lt;= 1.5.22 &#8211; Cross-Site Scripting Almacenado Autenticado (Contributor+) a través del shortcode videowhisper_picture_upload_guest	Internas	Passa sumo
Jet Engine &lt;= 3.6.2 &#8211; Cross-Site Scripting almacenado autenticado (Contributor+) a través del parámetro list_tag	Internas	Passa sumo
CVE-2023-6223	Internas	Passa sumo
CVE-2023-6498	Internas	Passa sumo
CVE-2023-6506	Internas	Passa sumo
CVE-2023-6520	Internas	Passa sumo
CVE-2023-6524	Internas	Passa sumo
CVE-2023-6567	Internas	Passa sumo
CVE-2023-6600	Internas	Passa sumo
CVE-2023-6629	Internas	Passa sumo
CVE-2023-6699	Internas	Passa sumo
CVE-2023-6733	Internas	Passa sumo
CVE-2023-6738	Internas	Passa sumo
CVE-2023-6747	Internas	Passa sumo
CVE-2023-6776	Internas	Passa sumo
CVE-2023-6828	Internas	Passa sumo
CVE-2023-6883	Internas	Passa sumo
CVE-2023-6980	Internas	Passa sumo
CVE-2023-6981	Internas	Passa sumo
CVE-2023-6984	Internas	Passa sumo
CVE-2023-7027	Internas	Passa sumo
CVE-2023-7068	Internas	Passa sumo

Ligações para a própria página

CVE-2023-51410	Internas	Passa sumo
CVE-2023-51418	Internas	Passa sumo
CVE-2023-51678	Internas	Passa sumo
CVE-2023-52177	Internas	Passa sumo
CVE-2024-0201	Internas	Passa sumo
CVE-2024-0616	Internas	Passa sumo
CVE-2024-5226	Internas	Passa sumo
CVE-2024-5260	Internas	Passa sumo
CVE-2024-5545	Internas	Passa sumo
CVE-2024-5668	Internas	Passa sumo
CVE-2024-6568	Internas	Passa sumo
CVE-2024-6709	Internas	Passa sumo
CVE-2024-6770	Internas	Passa sumo
CVE-2024-6824	Internas	Passa sumo
CVE-2024-6870	Internas	Passa sumo
CVE-2024-7032	Internas	Passa sumo
CVE-2024-7150	Internas	Passa sumo
CVE-2024-7257	Internas	Passa sumo
CVE-2024-7291	Internas	Passa sumo
CVE-2024-7390	Internas	Passa sumo
CVE-2024-7548	Internas	Passa sumo
CVE-2024-7651	Internas	Passa sumo
CVE-2024-7848	Internas	Passa sumo
CVE-2024-7854	Internas	Passa sumo
CVE-2024-43343	Internas	Passa sumo

Palavras-chave SEO

Núvem de palavras-chave

Palavras-chave SEO



wordpress vulnerabilidade para scripting através almacenado del january plugin cross-site

Consistência das Palavras-chave

Palavra-chave	Conteúdo	Título	Palavras-chave	Descrição	Cabeçalhos
wordpress	18	✓	✗	✓	✓
vulnerabilidade	17	✓	✗	✓	✓
cross-site	17	✗	✗	✗	✓
plugin	16	✗	✗	✗	✓
january	15	✗	✗	✗	✗

Usabilidade

	Url	Domínio : seguridadwordpress.es Cumprimento : 21
	Favicon	Ótimo, o site tem um favicon.
	Facilidade de Impressão	Não encontramos CSS apropriado para impressão.
	Língua	Otimo! A língua declarada deste site é en.
	Dublin Core	Esta página não tira vantagens do Dublin Core.

Documento

	Tipo de Documento	HTML 5
--	-------------------	--------

Documento

	Codificação	Perfeito. O conjunto de caracteres UTF-8 está declarado.
	Validação W3C	Erros : 0 Avisos : 0
	Privacidade do Email	Boa! Nenhum endereço de email está declarado sob a forma de texto!
	HTML obsoleto	Fantástico! Não detetámos etiquetas HTML obsoletas.
	Dicas de Velocidade	<ul style="list-style-type: none">✓ Excelente, este site não usa tabelas dentro de tabelas.✗ Oh não, o site usa estilos CSS nas etiquetas HTML.✗ Oh, não! O site utiliza demasiados ficheiros CSS (mais que 4).✓ Perfeito, o site usa poucos ficheiros JavaScript.✗ Atenção, o site não tira vantagem da compressão gzip.

Dispositivos Móveis

	Otimização para dispositivos móveis	<ul style="list-style-type: none">✓ Icon Apple✓ Meta Viewport Tag✓ Conteúdo Flash
--	-------------------------------------	---

Otimização

	XML Sitemap	Perfeito, o site tem um mapa XML do site (sitemap). http://seguridadwordpress.es/sitemap.xml
	Robots.txt	http://seguridadwordpress.es/robots.txt Perfeito, o seu site tem um ficheiro robots.txt.
	Analytics	Em falta Não detetámos nenhuma ferramenta analítica de análise de atividade. Este tipo de ferramentas (como por exemplo o Google Analytics)

Otimização

permite perceber o comportamento dos visitantes e o tipo de atividade que fazem. No mínimo, uma ferramenta deve estar instalada, sendo que em algumas situações mais do que uma pode ser útil.