INDICE

[**Objetivo** 2](#_Toc164875375)

[**Conclusiones** 2](#_Toc164875376)

[**Metodología** 2](#_Toc164875377)

[Introducción 2](#_Toc164875378)

[Buenas Prácticas de seguridad WordPress 2](#_Toc164875379)

[**Análisis de Vulnerabilidades** 3](#_Toc164875380)

[Ejecución de Análisis de vulnerabilidades 3](#_Toc164875381)

[Matriz de Riesgo 3](#_Toc164875382)

[Vulnerabilidades Encontradas 4](#_Toc164875383)

[Evidencia 5](#_Toc164875384)

[**Referencias** 5](#_Toc164875385)

[Metodológicas 5](#_Toc164875386)

[Tecnológicas 5](#_Toc164875387)

[Escaneo de Vulnerabilidades WordPress 5](#_Toc164875388)

[**Glosario** 6](#_Toc164875389)

# **Objetivo**

Realizar un análisis detallado de la tienda en línea (<https://challenge.mp-sec.org/>) con la finalidad de identificar posibles casos de abuso y riesgos de seguridad.

Esta revisión alcanza análisis debe incluir, pero no limitarse a, la revisión de la configuración de

WordPress y WooCommerce, como también plugins implementados en la solución.

En base al análisis previo, se diseñaron y ejecutaron casos de uso para verificar si los riesgos identificados son explotables y en función de esto se realizan recomendación de mitigación de cada hallazgo encontrado, como así también una valoración del riesgo incurrido para determinar su impacto y criticidad.

# **Conclusiones**

Luego de haber realizado un análisis profundo de todas las vulnerabilidades conocidas para las instancias WordPress, se determina que el sitio “Tienda” (<https://challenge.mp-sec.org/>) presenta un **nivel de riesgo** CRTICO **de ser vulnerado**.

Se requiere que se implementen las medidas correctivas que se destallan en el campo mitigación del apartado “Vulnerabilidades Encontradas” de este documento.

# **Metodología**

## Introducción

Se tomo como marco de referencia OWASP Top 10 (<https://owasp.org/www-project-top-ten/>) , una guía estándar del sector que enumera los riesgos más críticos para la seguridad de las aplicaciones.

En base a este marco referencial se instanciaron las mejores practicas aplicables a este tipo de aplicación gestoras de contenido, CMS (Content Manager Sistems), las cuales cuentan con lineamientos de seguridad de código y pruebas de vulnerabilidades muy bien controladas. ([Seguridad – Servicio de soporte WordPress.com](https://wordpress.com/es/support/seguridad/)).

Iniciamos con un escaneo sobre la instancia <https://challenge.mp-sec.org/> utilizando WPScan, una herramienta específica para escanear vulnerabilidades de WordPress (<https://wpscan.com/>), la cual cuenta con una base de datos de todas las vulnerabilidades reportadas para WordPress (<https://wpscan.com/api>), sobre el resultante de este escaneo, se analizaron todas aquellas revisiones que no fueron 100% satisfactorias y se crearon casos de pruebas para intentar vulnerarlas.

Adicionalmente, se incluyeron revisiones de buenas prácticas de seguridad WordPress.

## Buenas Prácticas de seguridad WordPress

* Versión de WordPress
* Temas y plugins de terceros
* Backdoors (Puertas traseras)
* Autenticación de usuario débil
* Configuraciones predeterminadas de WordPress
  + Panel Login / Backoffice solo accesible a IP’s específicas.
  + Xmlrpc.php, este servicio es el CORE de WordPress.
  + Cron.php servicio vulnerable a ataques DDOS (Denegación de Servicios).
  + wp-config.php, información confidencial del sitio.

# **Análisis de Vulnerabilidades**

Se ejecutaron una serie de revisiones de seguridad sobre las vulnerabilidades encontradas en el escaneo previo, se estableció un nivel de riesgo para cada una según su criticidad, tomando como vector la matriz de riesgo definida en el apartado “Matriz de Riesgo” y por último se propone una acción de mitigación.

## Ejecución de Análisis de vulnerabilidades

Se ejecuto el escaneo en “Modo Agresivo”, donde el escaneo intrusivo ejecutado por WPscan será más profundo y enviará cientos de solicitudes al servidor para encontrar vulnerabilidades, si las hay, en todos los plugins de WordPress.



## Matriz de Riesgo

|  |  |
| --- | --- |
| NIVEL | CRITICIDAD |
| CRITICO | Un estado de riesgo crítico indica que un sistema tiene un riesgo severo e inmediato de eventos destructivos. Estos eventos incluyen ataques cibernéticos o fallas de equipos que, si no se abordan, provocarían interrupciones generalizadas, violaciones importantes de información o cierres del sistema.  Estos riesgos también tienen una alta probabilidad de ocurrir en un futuro muy cercano. |
| ALTO | Un alto riesgo de ciberseguridad significa que existe una posibilidad inmediata de que se produzcan eventos dañinos que puedan comprometer los sistemas. El riesgo alto es un paso por debajo del riesgo crítico, pero aún indica eventos perjudiciales o disruptivos de alto impacto.  Los eventos de alto riesgo también indican una alta probabilidad de explotación, daño o interrupción si los problemas no se abordan rápidamente. |
| MEDIO | El riesgo de ciberseguridad medio significa que existe la posibilidad de actividad maliciosa. Los niveles de daño potencial son moderados, pero no graves.  Si bien no es perjudicial de inmediato, un evento de riesgo medio puede convertirse en un riesgo grave si no se aborda. |
| BAJO | El bajo riesgo de ciberseguridad significa que hay pocas anomalías fuera de la preocupación habitual por los eventos de ciberdelito.  En un estado de bajo riesgo, la actividad de su red se considera normal. No se están produciendo eventos importantes o peligrosos en su sistema. Si se detecta un problema, suele ser pequeño y fácil de solucionar. |

## Vulnerabilidades Encontradas

|  |  |  |  |
| --- | --- | --- | --- |
| Vulnerabilidad | Detalle | Riesgo | Mitigación |
| Backdoor | Se encuentra expuesto el panel de administración de la plataforma (wp-admin) lo cual compromete gravemente la seguridad de la instancia, dado que, si un atacante logra accederlo, tendría la capacidad de controlar todas las funcionalidades del sistema como así también acceder a datos sensibles.  **Evidencia** <https://challenge.mp-sec.org/wp-login.php> | CRITICO | Limitar el acceso al wp-admin basado en la IP.   Es recomendado cambiar la URL de acceso por defecto del wp-admin (backoffice).  **Referencia**:  [Restringir Acceso a Admin WP](https://blog.infranetworking.com/restringir-acceso-panel-administrador-wordpres-por-ip-o-usuario/) |
| XML-RPC seems to be enabled | La exposición de este servicio compromete seriamente la seguridad de la instancia ya que permite interactuar remotamente con el sitio.  Existen 2 debilidades principales:   * La primera es usar ataques de fuerza bruta para obtener acceso a tu sitio. * La segunda era desactivar sitios a través de un ataque DDoS.   **Evidencia** <https://challenge.mp-sec.org/xmlrpc.php> | CRITICO | Deshabilitar o bien restringir el acceso al servicio solo para autorizados.  **Referencia**:  [Deshabiiltar Xmlrpc.php](https://www.hostinger.com.ar/tutoriales/que-es-xmlrpc-php-wordpress-por-que-desactivarlo/?ppc_campaign=google_search_generic_hosting_all&bidkw=defaultkeyword&lo=1000073&gad_source=1&gclid=CjwKCAjw26KxBhBDEiwAu6KXt7zzbvMsWClLRJ0EuISMSB97bbro6wjUCXatww3ZQgFWgvtNQuRg3xoCEeEQAvD_BwE) |
| Archivos de Instalación no eliminados | Si bien podría no ser tomado como una vulnerabilidad, la exposición de estos archivos de instalación, podrían proporcionar de información utilizable para los atacantes.  **Evidencia**  <https://challenge.mp-sec.org/wp-admin/install.php>  <https://challenge.mp-sec.org/readme.html> | MEDIO | Es recomendado eliminar con celeridad los archivos de instalación detallados en este hallazgo. |
| BAJO |
| The external WP-Cron seems to be enabled | https://challenge.mp-sec.org/wp-cron.php | MEDIO | **Referencias**:   * [Ref. 1](https://www.iplocation.net/defend-wordpress-from-ddos) * [Ref. 2](https://github.com/wpscanteam/wpscan/issues/1299) |

## **Evidencia**

|  |  |
| --- | --- |
| Descripcion | Adjunto |
| Escaneo de Vulnerabilidades WPScan |  |
| Ataques Ejecutados   * Searching for XML-RPC servers on WordPress * Brute force attacks * XML-RPC pingbacks attacks   + Distributed denial-of-service (DDoS) attacks   + Cloudflare Protection Bypass (find real server ip)   + XSPA (Cross Site Port Attack) |  |

# **Referencias**

Material utilizado como referencia para la ejecución de este informe.

## Metodológicas

* [OWASP Top Ten | OWASP Foundation](https://owasp.org/www-project-top-ten/)
* [Seguridad – Servicio de soporte WordPress.com](https://wordpress.com/es/support/seguridad/)
* [WORDPRESS - Análisis y vulnerabilidades | PARTE I - YouTube](https://www.youtube.com/watch?v=hlfMJI9vp0c&t=327)
* [WORDPRESS - Análisis y vulnerabilidades | PARTE II - YouTube](https://www.youtube.com/watch?v=JtbB0msDP1s)
* [Guía para Restringir acceso al panel administrador WordPress (infranetworking.com)](https://blog.infranetworking.com/restringir-acceso-panel-administrador-wordpres-por-ip-o-usuario/)
* [Las 10 principales vulnerabilidades de OWASP - Check Point Software](https://www.checkpoint.com/es/cyber-hub/cloud-security/what-is-application-security-appsec/owasp-top-10-vulnerabilities/)

## Tecnológicas

* [WooCommerce](https://woocommerce.com/es/)
* [WooCommerce - WooCommerce - Mercado Pago Developers](https://www.mercadopago.cl/developers/es/docs/woocommerce/introduction)

## Escaneo de Vulnerabilidades WordPress

* [WPScan: WordPress Security Scanner](https://wpscan.com/)
* [WordPress Vulnerability Database API | WPScan](https://wpscan.com/api/)
* [Installing WPScan | WPScan](https://wpscan.com/blog/wpscan-user-documentation/)
* [WPScan WordPress Security Scanner | LinkedIn](https://www.linkedin.com/pulse/wpscan-wordpress-security-scanner-charlie-m-/)
* [Comprueba la seguridad de tu Wordpress - LBT (lobobrothers.com)](https://tech.lobobrothers.com/comprueba-la-seguridad-de-tu-wordpress/)
* [Instale WPScan WordPress Security Scanner en Ubuntu 20.04 LTS - FastWebLaunch](https://fastweblaunch.com/blog/instale-wpscan-wordpress-security-scanner-en-ubuntu-20-04-lts/)

# **Glosario**

|  |  |
| --- | --- |
| Término | Definición |
| Versión de WordPress | WordPress actualiza regularmente su software principal para revisar las vulnerabilidades existentes y reforzar sus defensas contra las amenazas emergentes. Las versiones antiguas de WordPress no tienen estas protecciones y pueden seguir siendo susceptibles de sufrir ataques. |
| Temas y plugins de terceros | Los temas y plugins de WordPress de terceros ofrecen una amplia gama de funcionalidades, pero no siempre cumplen con los requisitos de seguridad más recientes. Como tales, pueden crear riesgos cuando se instalan en un sitio de WordPress. |
| Backdoors (Puertas traseras) | Este tipo de vulnerabilidad permite que el atacante que ha accedido a una cuenta WordPress se pueda crear una “puerta trasera”, un método encubierto para eludir las medidas de seguridad. Los backdoors permiten que el atacante acceda repetidamente a un sitio WordPress o lanzar nuevos ataques. |
| Autenticación de usuario débil | No practicar una higiene adecuada de las contraseñas (crear contraseñas seguras, cambiar regularmente las contraseñas, etc.) o no implementar la autenticación de múltiples factores (MFA) puede aumentar el riesgo de una fuga. |
| Configuraciones predeterminadas de WordPress | WordPress tiene varios ajustes predeterminados que facilitan al atacante la identificación de puntos de entrada comunes. |
| WordPress | WordPress es una plataforma de gestión de contenidos, representa un software de código abierto altamente versátil que permite a los usuarios crear y desarrollar sitios web personalizados de manera sencilla, adaptable y profesional, con una muy buena experiencia de usuario. |
| WooCommerce | Plugin de comercio electrónico para WordPress que permite la creación de tiendas en línea para pequeñas y grandes empresas |
| Plugin | Los plugins son complementos que añaden funcionalidades extra o mejoras a los programas. Es decir, son mini programas que suman alguna característica que no venía por defecto en el programa original. Funcionan como añadidos, pero no por sí mismos. |
| OWASP (Open Web Application Security Project) | Metodología de seguridad de auditoría web, abierta y colaborativa, orientada al análisis de seguridad de aplicaciones Web, y usada como referente en auditorías de seguridad. |
| CMS (Content Manager Sistems) | CMS son las siglas de Content Management System (Sistema de Gestión de Contenidos). De modo que, en pocas palabras, un CMS es una herramienta que ayuda a las empresas a crear, publicar y gestionar el contenido de sus páginas web |
| WPScan | Herramienta de código abierto que permite analizar la seguridad de cualquier sitio web desarrollado en WordPress, propio o de terceros, dispone del listado actualizado de vulnerabilidades reportadas para la plataforma. |
| IP | Una dirección IP es una dirección única que identifica a un dispositivo en Internet o en una red local. IP significa “protocolo de Internet”, que es el conjunto de reglas que rigen el formato de los datos enviados a través de Internet o la red local.  En esencia, las direcciones IP son el identificador que permite el envío de información entre dispositivos en una red. Contienen información de la ubicación y brindan a los dispositivos acceso de comunicación. Internet necesita una forma de diferenciar entre distintas computadoras, enrutadores y sitios web. Las direcciones IP proporcionan una forma de hacerlo y forman una parte esencial de cómo funciona Internet. |
| DDoS (Distributed Denial of Service) | Un ataque de DDoS, o denegación de servicio distribuido, es un intento malintencionado de interrumpir el tráfico en un servidor, servicio o red, abrumando al objetivo o a su infraestructura circundante con una inundación de tráfico de internet.  Los ataques de DDoS coordinan una gran cantidad de sistemas informáticos comprometidos para crear tráfico atacante. Los equipos abusados incluyen ordenadores y otros recursos con conexión a redes, como dispositivos IoT. |