



# Casbeep

Ciberseguridad para autónomos y micropymes

---

## **Informe de Vulnerabilidades WordPress Agosto 2020**

Hola,

En este pequeño informe no me voy a entretener mucho.

Mi intención es que tengas de forma resumida **lo que ha ocurrido en cuanto a seguridad en WordPress se refiere en todo un mes.**

En cualquier caso, espero que lo disfrutes y puedas aprender algo y que digas: “pues mira, mereció la pena”.

Lógicamente, no es un servicio a medida, ni un curso, ambas cosas tendrían un precio y una intensidad de trabajo muy diferentes.

Aquí como ves te estoy regalando algo que podría ser perfectamente una sección de uno de mis servicios.

En todo caso, esta es una manera muy efectiva de empezar a entender que tipo de vulnerabilidades puedes encontrarte en WordPress, plugins y themes.

---

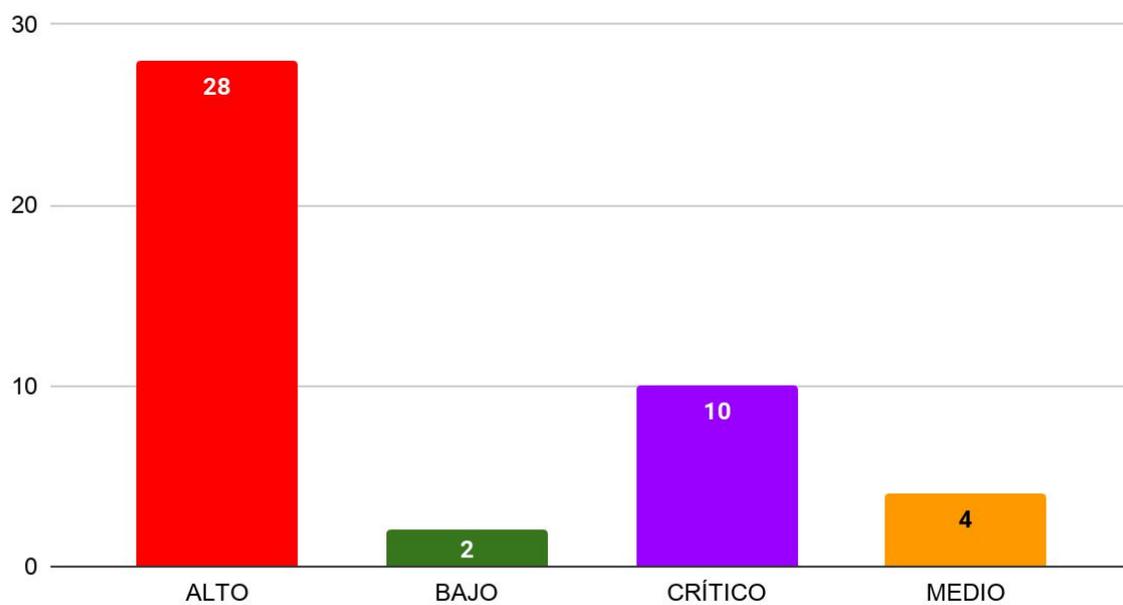
## Vulnerabilidades en el núcleo

Este mes no se han publicado vulnerabilidades en el núcleo de WordPress pero sí que se ha publicado una nueva rama, la 5.5.

## Vulnerabilidades en Plugins

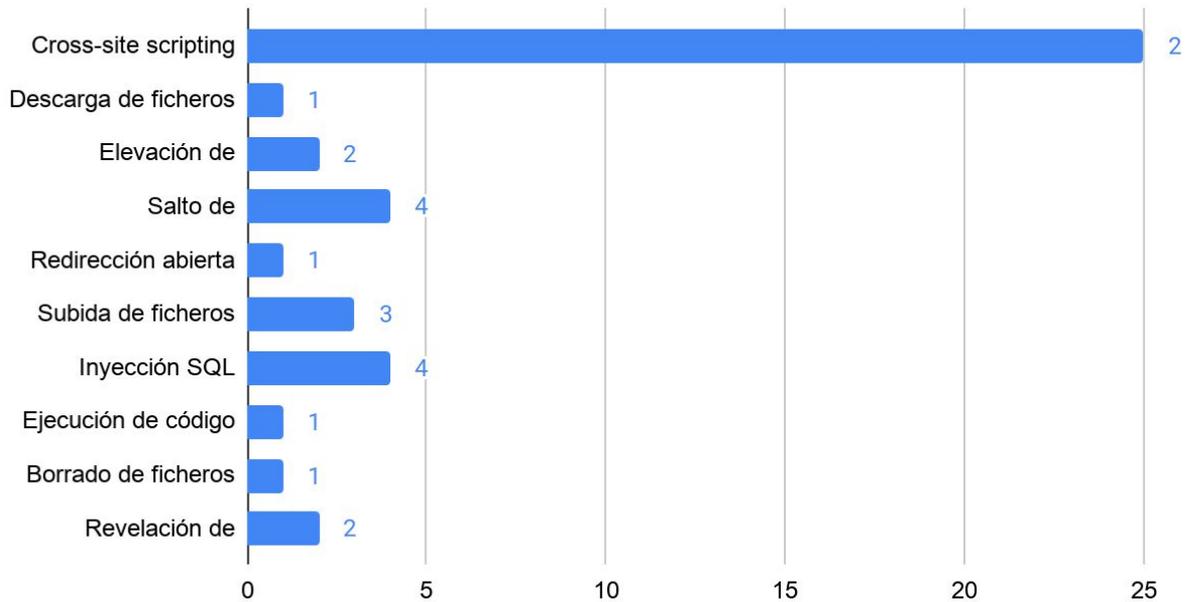
En el siguiente gráfico puedes ver el número total de vulnerabilidades detectadas junto a su clasificación por riesgo.

Clasificación por impacto



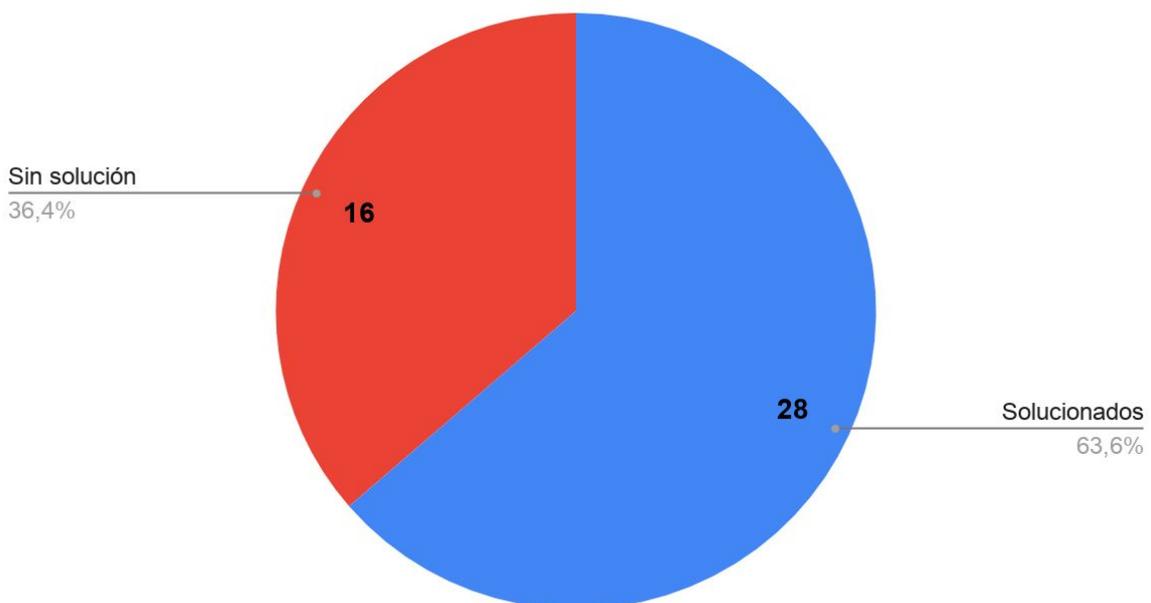
En el siguiente gráfico puedes ver el número total de vulnerabilidades detectadas junto a su clasificación por tipo.

### Clasificación por tipo



En el siguiente gráfico puedes ver el número total de vulnerabilidades detectadas junto a su clasificación por riesgo.

### Sin solución frente a Solucionados



---

## Autoptimize

Vulnerabilidad	Nivel de impacto	Solución
Subida de ficheros	CRÍTICO	2.7.7

## Advanced Access Manager

Vulnerabilidad	Nivel de impacto	Solución
Elevación de privilegios	CRÍTICO	6.6.2

## Cardoza WordPress Poll

Vulnerabilidad	Nivel de impacto	Solución
Inyección SQL	CRÍTICO	N/A

## Discount Rules for WooCommerce

Vulnerabilidad	Nivel de impacto	Solución
Inyección SQL	CRÍTICO	2.1.0

## Divi Builder

Vulnerabilidad	Nivel de impacto	Solución
Subida de ficheros	CRÍTICO	4.5.3

---

## Newsletter

Vulnerabilidad	Nivel de impacto	Solución
Ejecución de código	CRÍTICO	6.8.2

## Quiz and Survey Master

Vulnerabilidad	Nivel de impacto	Solución
Subida de ficheros	CRÍTICO	7.0.1
Borrado de ficheros	CRÍTICO	7.0.1

## Recall Products

Vulnerabilidad	Nivel de impacto	Solución
Inyección SQL	CRÍTICO	N/A

## RSVPMaker

Vulnerabilidad	Nivel de impacto	Solución
Inyección SQL	CRÍTICO	7.8.2

---

## Admin Menu

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	N/A

## Bulk Change

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	N/A

## Ceceppa Multilingua

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	N/A

## Change WordPress Login Logo

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	N/A

## Click to top

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	N/A

---

## Discount Rules for WooCommerce

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	2.1.0

## Easy Media Download

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	1.1.5

## Elegant Testimonial

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	N/A

## FooGallery

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	1.9.25

## Internal Links Manager

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	N/A

---

## Newsletter

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	6.8.2

## NextGEN Gallery Sell Photo

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	N/A

## Product Input Fields for WooCommerce

Vulnerabilidad	Nivel de impacto	Solución
Descarga de ficheros	ALTO	1.2.7

## Recall Products

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	N/A

## Responsive Lightbox2

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	1.0.3

---

## RSS Feed Widget

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	2.8.1

## Sell Media

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	2.4.2

## Sell Photo

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	N/A

## Subscribe Sidebar

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	N/A

## The Official WordPress Facebook Chat Plugin

Vulnerabilidad	Nivel de impacto	Solución
Elevación de privilegios	ALTO	1.6

---

## Ultimate Appointment Booking & Scheduling

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	1.1.10

## Very Simple Quiz

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	N/A

## WooCommerce – NAB Transact

Vulnerabilidad	Nivel de impacto	Solución
Salto de restricciones	ALTO	2.1.2

## WordPress Colorbox Lightbox

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	N/A

## WordPress fancyBox Lightbox

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	1.0.2

---

## WP Customer Reviews

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	3.4.3

## WP Floating Menu

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	1.4.1

## WP Smart CRM

Vulnerabilidad	Nivel de impacto	Solución
Cross-site scripting	ALTO	N/A

---

## Advanced Access Manager

Vulnerabilidad	Nivel de impacto	Solución
Revelación de información	MEDIO	6.6.2

## CMP - Coming Soon & Maintenance

Vulnerabilidad	Nivel de impacto	Solución
Salto de restricciones	MEDIO	3.8.2

## File Manager

Vulnerabilidad	Nivel de impacto	Solución
Revelación de información	MEDIO	6.5

## Kali Forms

Vulnerabilidad	Nivel de impacto	Solución
Salto de restricciones	MEDIO	2.1.2

---

## Discount Rules for WooCommerce

Vulnerabilidad	Nivel de impacto	Solución
Salto de restricciones	BAJO	2.1.0

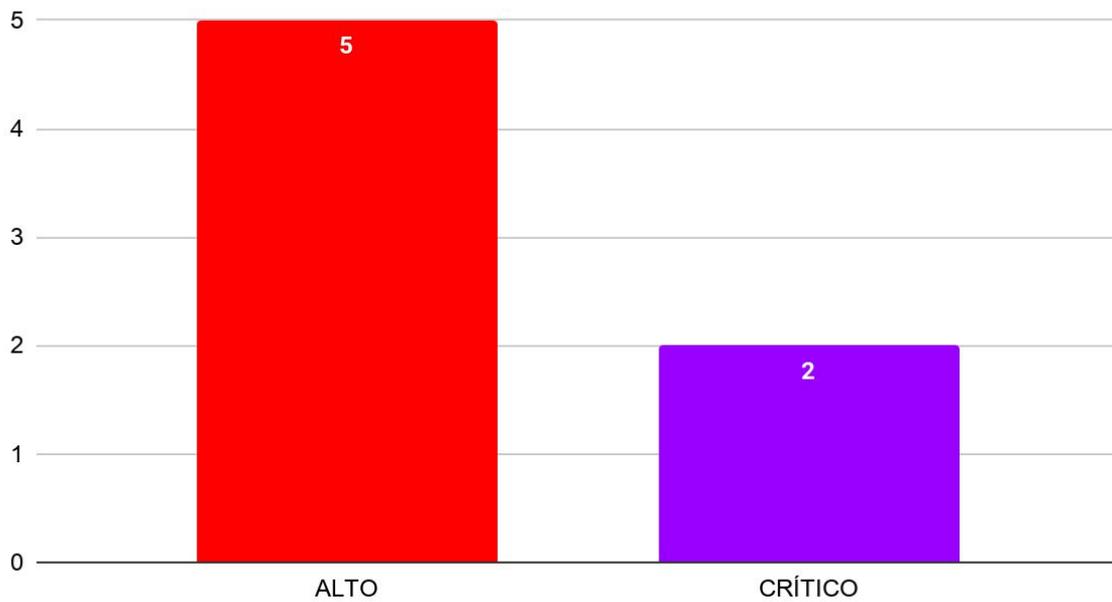
## Ultimate Member

Vulnerabilidad	Nivel de impacto	Solución
Redirección abierta	BAJO	2.1.7

## Vulnerabilidades en Themes

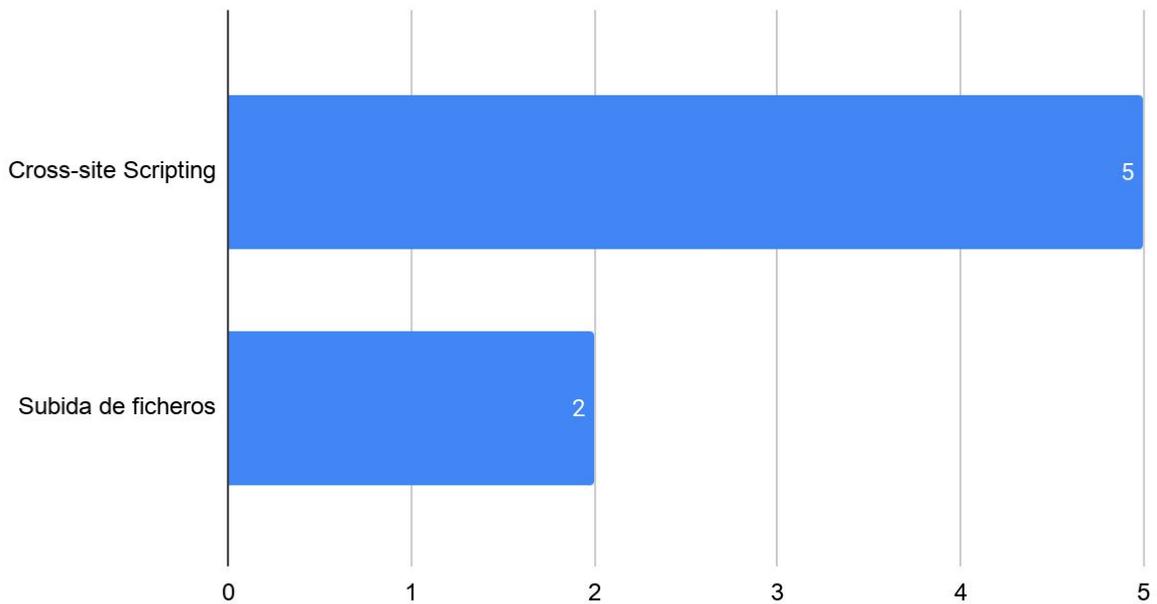
En el siguiente gráfico puedes ver el número total de vulnerabilidades detectadas junto a su clasificación por riesgo.

Clasificación por impacto



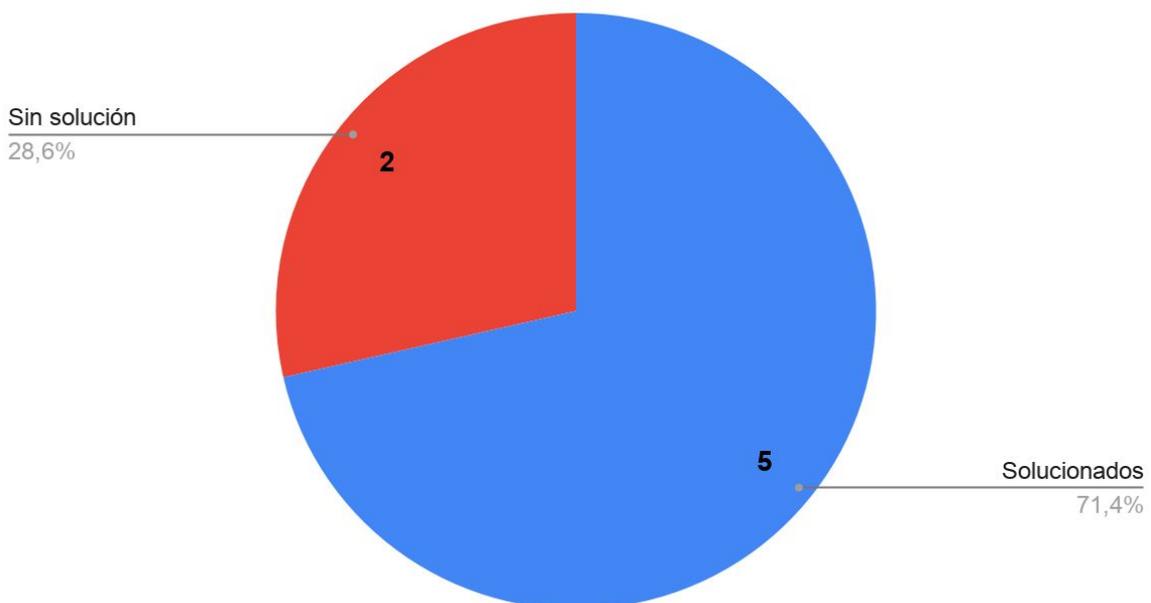
En el siguiente gráfico puedes ver el número total de vulnerabilidades detectadas junto a su clasificación por tipo.

### Clasificación por tipo



En el siguiente gráfico puedes ver el número total de vulnerabilidades detectadas junto a su clasificación por riesgo.

### Sin solución frente a Solucionados



---

## Divi

Vulnerabilidad	Nivel de impacto	Solución
Subida de ficheros	CRÍTICO	4.5.3

## Extra

Vulnerabilidad	Nivel de impacto	Solución
Subida de ficheros	CRÍTICO	4.5.3

## FoodBakery

Vulnerabilidad	Nivel de impacto	Solución
Cross-site Scripting	ALTO	2.0

## Konzept

Vulnerabilidad	Nivel de impacto	Solución
Cross-site Scripting	ALTO	2.5

## Nova Lite

Vulnerabilidad	Nivel de impacto	Solución
Cross-site Scripting	ALTO	1.3.9

---

## Home Villas

Vulnerabilidad	Nivel de impacto	Solución
Cross-site Scripting	ALTO	N/A

## Geo Magazine

Vulnerabilidad	Nivel de impacto	Solución
Cross-site Scripting	ALTO	N/A

Bueno, ya hemos llegado al final.

Espero que le saques mucho partido a este informe que he querido regalarte.

Y sobre todo, veas la seguridad con otros ojos.

Que pases un buen día.

Fernando Castillo.

**PD:** No olvides leer los emails que mando. Siempre puede caer algún regalito más.