Auditoría de Seguridad Web

Análisis WordPress Inteligente

test-url.com

NIVEL DE RIESGO GLOBAL

CRÍTICO

FECHA	TIPO	ANALISTA
25/01/2026	**Informe Ejecutivo**	iAPentest

Resumen de Hallazgos

Análisis automatizado de seguridad WordPress

4	1	4	0
CRÍTICOS	ALTOS	MEDIOS	BAJOS

1. Resumen ejecutivo

Este análisis pasivo, no intrusivo, realiza una identificación rápida de vulnerabilidades conocidas y áreas de mejora relacionadas con la seguridad, estabilidad y cumplimiento normativo del sitio. El informe resume los puntos clave de forma ejecutiva.

Nivel de riesgo global estimado: CRÍTICO

El sitio analizado presenta un total de **9 hallazgos**: 4 críticos, 1 altos, 4 medios y 0 bajos.

💡 **Para obtener el análisis exhaustivo de todos los componentes**, incluyendo detección completa de plugins/temas, biblioteca de casos reales en función de los hallazgos, matriz de riesgos (probabilidad/impacto), instrucciones de remediación paso a paso, etc., solicite el **Informe Técnico (Pack CORE - 249€, lanzamiento 179€)**.

2. Top 5 Riesgos Clave

Los siguientes hallazgos representan los riesgos más significativos detectados, ordenados por severidad e impacto potencial en el negocio.

1. **Exposición de Usuarios:** API REST expone 2 usuarios: `admin_webmaster`, `javier_marketing`
2. **Versión PHP:** PHP 7.4 sin soporte desde 2022-11-28. PHP sin soporte activo
3. **Vulnerabilidades Conocidas:** Detectada(s) 11 vulnerabilidad(es) en componentes instalados (CVE-2022-2267, CVE-2022-2556, CVE-2024-39666)
4. **Protección HTTP:** Cabeceras de seguridad críticas no implementadas
5. **Versión WordPress:** WordPress 6.5.7 desactualizado (actual: 6.9)

3. Impacto en el negocio

- **Riesgo económico:** Coste potencial de limpieza de malware (500-3.000€), recuperación de SEO (1.200-6.000€), pérdida de ventas durante caída del servicio (300-12.000€+).
- **Reputación:** Daño a la imagen de marca si el sitio es comprometido. El impacto reputacional es difícil de cuantificar pero puede ser devastador para el negocio.
- **Legal:** Posibles sanciones RGPD por exposición de datos personales (900€ - 10.000€+ según gravedad).
- **Seguridad:** El sitio puede ser comprometido por atacantes automatizados. Coste medio de un ciberataque a PYMES españolas: 35.000€ (INCIBE 2024).
- **Disponibilidad:** Riesgo de caída del servicio por ataques. El 60% de las PYMES que sufren un ciberataque cierran en los 6 meses siguientes.

4. Diagnóstico iAPentest

🤖 Análisis experto generado por inteligencia artificial especializada en ciberseguridad WordPress.

El sistema correlaciona múltiples puntos de verificación, cruza hallazgos entre módulos para identificar riesgos reales en contexto global, prioriza acciones según impacto y probabilidad, y selecciona casos reales relacionados con las evidencias detectadas en tu sitio.

Su sitio web presenta un **nivel de riesgo CRÍTICO** con una puntuación de 57/100, evidenciando **4 vulnerabilidades críticas** y 1 de alto riesgo que comprometen seriamente la seguridad. Los hallazgos incluyen **11 vulnerabilidades CVE** documentadas, **PHP 7.4 obsoleto** sin soporte desde 2022, y **cabeceras de seguridad críticas ausentes** como content-security-policy.

La situación se agrava por la combinación de factores: la **API REST /wp-json/wp/v2/users expone 2 usuarios** (admin_webmaster, javier_marketing) facilitando ataques de fuerza bruta dirigidos, mientras que el **stack tecnológico desactualizado** (Apache + PHP 7.4.33 + WordPress 6.5.7) amplifica exponencialmente el riesgo de explotación exitosa de las vulnerabilidades detectadas.

La combinación de usuarios expuestos, software obsoleto y múltiples CVEs activos requiere **atención urgente**. Recomendamos implementar el **pack SHIELD Advanced** y actuar cuanto antes en la actualización del entorno tecnológico para mitigar estos riesgos críticos.

El Coste de NO Actuar

Comparativa entre el coste de remediación preventiva vs el coste promedio de un incidente de seguridad.

✅ **Remediación AHORA**

750€

Pack SHIELD Advanced

- ✅ Corrección de hallazgos
- 🛠️ Mejoras técnicas incluidas
- 🤝 Remediación delegada
- 📄 Informe Antes/Después

vs

❌ **Coste de Incidente**

3.000€-10.000€+

- 💰 Limpieza malware: 500-3.000€
- 📉 Pérdida ventas: 300-12.000€+
- 🔍 Recuperación SEO: 1.200-6.000€+
- ⚖️ Sanciones RGPD: 900-10.000€+
- 😨 Daño reputación: incalculable

> **Fuente:** El coste medio de un ciberataque a PYMES españolas es de 35.000€ y el 60% cierra en 6 meses.
> *(INCIBE / Vodafone Business 2024)*

5. Casos reales relacionados con los hallazgos (2023-2025)

Nota: A continuación mostramos casos reales relacionados con los **hallazgos detectados** en este análisis. Los casos se seleccionan dinámicamente según los riesgos identificados para proporcionar contexto relevante y específico.

1. Ransomware paraliza durante semanas el Ayuntamiento de Cangas (Pontevedra), afectando nóminas, catastro y Policía Local.

Cifrado masivo de sistemas municipales y pérdida temporal de acceso a aplicaciones clave. Grave impacto en la ciudadanía, retrasos administrativos y posible responsabilidad por mala gestión de la seguridad.

Impacto: Cifrado masivo de sistemas municipales y pérdida temporal de acceso a aplicaciones clave. Grave impacto en la ciudadanía, retrasos administrativos y posible responsabilidad por mala gestión de la seguridad.

Año: 2023 | **Fuente:** El País + informes CEN – ciberataque Ayuntamiento de Cangas (LockBit)

2. Vulnerabilidad en múltiples ramas de WordPress (CVE-2023-39999) permite exposición de información confidencial.

Posible acceso a datos internos en instalaciones sin parchear. Sitios sin actualizar quedan expuestos a robo de información y posteriores movimientos laterales.

Impacto: Posible acceso a datos internos en instalaciones sin parchear. Sitios sin actualizar quedan expuestos a robo de información y posteriores movimientos laterales.

Año: 2023 | **Fuente:** INCIBE-CERT – alerta temprana CVE-2023-39999

3. Plugin WooCommerce Easy Duplicate Product presenta XSS reflejado sin autenticación (CVE-2023-30747).

Posibilidad de ejecutar Javascript malicioso en navegadores de usuarios que visitan URLs manipuladas. Riesgo de robo de sesiones, datos de clientes o redirecciones a sitios fraudulentos.

Impacto: Posibilidad de ejecutar Javascript malicioso en navegadores de usuarios que visitan URLs manipuladas. Riesgo de robo de sesiones, datos de clientes o redirecciones a sitios fraudulentos.

Año: 2023 | **Fuente:** INCIBE-CERT – CVE-2023-30747

4. MingoCommerce WooCommerce Product Inquiry presenta XSS almacenado no autenticado (CVE-2023-32796).

Atacantes pueden inyectar contenido persistente en la tienda sin autenticación. Compromiso de la confianza del cliente y posible robo de datos.

Impacto: Atacantes pueden inyectar contenido persistente en la tienda sin autenticación. Compromiso de la confianza del cliente y posible robo de datos.

Año: 2023 | **Fuente:** INCIBE-CERT – CVE-2023-32796

Fuentes documentadas: Informes públicos de incidentes en WordPress, INCIBE-CERT, AEPD, estudios sectoriales de ciberseguridad, análisis de casos reales españoles 2023-2025.

6. Tabla de vulnerabilidades y priorización de riesgos

En la siguiente tabla se resumen los principales hallazgos detectados en la Fase I (análisis pasivo del perímetro público). El detalle técnico completo se desarrolla en el Informe Técnico asociado (previa solicitud) o, adicionalmente, con la contratación de los servicios de remediación.

Módulo	Hallazgo	Criticidad
Exposición de Usuarios	API REST expone 2 usuarios: `admin_webmaster`, `javier_marketing`	CRÍTICO
Versión PHP	PHP 7.4 sin soporte desde 2022-11-28. PHP sin soporte activo	CRÍTICO
Vulnerabilidades Conocidas	Detectada(s) 11 vulnerabilidad(es) en componentes instalados (CVE-2022-2267, CVE-2022-2556, CVE-2024-39666)	CRÍTICO
Protección HTTP	Cabeceras de seguridad críticas no implementadas	CRÍTICO
Versión WordPress	WordPress 6.5.7 desactualizado (actual: 6.9)	ALTO
Protección Login	No se detectó protección específica de login. Panel de administración expuesto a ataques de fuerza bruta.	MEDIO
Protección WAF	No se detectó WAF ni plugin de seguridad. Se recomienda instalar protección.	MEDIO
Exposición de Rutas	Rutas administrativas estándar expuestas en robots.txt.	MEDIO
Archivos Servidor	3 rutas con protección mejorable	MEDIO
Cumplimiento Legal	Cumplimiento legal correcto. Páginas legales completas con elementos obligatorios RGPD/LOPDGDD.	INFO
Plugins Problemáticos	Ningún plugin clasificado como crítico para rendimiento	INFO
Certificado SSL	Certificado expira en 31 días	INFO
Conexión Segura	Conexión segura correctamente configurada (HTTPS + HSTS)	INFO
Dependencias Externas	No se detectaron recursos externos	INFO
Ejecución PHP Directa	Ejecución de código PHP correctamente bloqueada en rutas de plugins	INFO
JavaScript Vulnerable	Todas las bibliotecas JavaScript detectadas (2) están actualizadas	INFO

Componentes WordPress Detectados

Se han identificado **12 plugins** y **3 temas** mediante análisis pasivo del frontend.

ℹ️ El listado de componentes puede no ser exhaustivo. Plugins de backend (seguridad, backups, administración) requieren acceso autenticado para su detección completa (Fase II - Auditoría autenticada: Análisis profundo con acceso al panel WordPress, bajo petición).

Componente	Tipo	Versión	Estado
WooCommerce	Plugin	9.1.1	⚠️ **8 CVE**
Mailchimp For Woocommerce	Plugin	N/A	**2 CVE**
All In One Wp Migration	Plugin	—	⚠️ Verificar
Classic Editor	Plugin	—	Verificar
Cookie Law Info	Plugin	—	Verificar
Dflip	Plugin	1.7.5.1	✓ OK
Duplicate Post	Plugin	—	Verificar
Google Site Kit	Plugin	—	Verificar
Starter Commerce	Plugin	4.7.2.9.2	✓ OK
Starter_Column_Layouts	Plugin	6.5.7	✓ OK
Wp Maintenance Mode	Plugin	—	Verificar
Wp Rocket	Plugin	—	⚠️ Verificar
Flavor Starter	Tema	4.26.0	⚠️ **1 CVE**
Flavor Starter	Tema	4.26.0	✓ OK
Test Url Theme	Tema	4.26.0	✓ OK

7. Matriz de riesgos

Distribución de hallazgos según probabilidad de ocurrencia e impacto potencial en el negocio.

	BAJO Impacto	**MEDIO** Impacto	**ALTO** Impacto	**CRÍTICO** Impacto
ALTA Probabilidad	—	—	—	*Protección HTTP* *Versión PHP* *Exposición de Usuarios* *Vulnerabilidades Conocidas*
MEDIA Probabilidad	—	—	*Archivos Servidor* *Exposición de Rutas* *Protección Login* *Protección WAF*	*Versión WordPress*
BAJA Probabilidad	—	—	—	—

Nota: La matriz muestra la distribución de hallazgos según su probabilidad de ocurrencia e impacto en el negocio. Los módulos restantes (bajos e informativos) no aparecen en la matriz por su bajo riesgo.

8. Recomendaciones inmediatas

Las siguientes acciones deben priorizarse según su nivel de criticidad. Se recomienda abordar primero los hallazgos críticos, seguidos de los altos.

🔴 Acción Prioritaria

1. 🔴 **Exposición de Usuarios:** Bloquear enumeración de usuarios
2. **Versión PHP:** Actualizar versión de PHP
3. **Vulnerabilidades Conocidas:** Revisar y corregir (múltiples protecciones pendientes)
4. 🔴 **Protección HTTP:** Implementar cabeceras de seguridad (múltiples protecciones pendientes)
5. 🟠 **Versión WordPress:** Actualizar WordPress a última versión

🟡 Mejoras Recomendadas

1. 🟡 **Protección Login:** Proteger acceso al panel de administración
2. **Protección WAF:** Instalar plugin de seguridad WAF
3. **Exposición de Rutas:** Minimizar información expuesta en robots.txt y sitemap (múltiples protecciones pendientes)
4. 🟡 **Archivos Servidor:** Proteger accesos (xmlrpc, wp-login) y eliminar exposiciones

💡 ***Nota:*** *Para detalles técnicos específicos sobre cómo implementar estas correcciones,* ***solicite el Informe Técnico (Pack CORE)****.*

Comparativa de Packs

Nuestros packs están diseñados para adaptarse a las necesidades de cada cliente, desde el diagnóstico inicial hasta la protección continua. Consúltenos.

Función	FREE	CORE	SHIELD	GUARDIAN(*)
Informe Ejecutivo	✔	✔	✔	✔
Informe Técnico	✘	✔	✔	✔
Remediación Delegada	✘	✘	✔	✔
Seguridad Gestionada	✘	✘	✘	✔

(*) GUARDIAN incluye todos los productos exclusivamente para contratación ANUAL. Para la opción MENSUAL sólo se realiza la función de «Seguridad Gestionada».

9. Alcance y notas finales

Alcance de la auditoría

- **Tipo:** Análisis pasivo y no intrusivo desde perímetro público
- **Metodología:** Recopilación de señales técnicas visibles sin autenticación
- **Sin acceso:** No se ha accedido al panel de administración ni al servidor
- **Sin impacto:** No se han realizado pruebas que puedan afectar al funcionamiento del sitio

Limitaciones

- Algunos riesgos internos solo son detectables con acceso autenticado
- Las versiones exactas de plugins pueden estar ocultas sin herramientas avanzadas
- La configuración interna del servidor no es visible externamente

Próximos pasos recomendados

1. **Solicitar Informe Técnico (Pack CORE):** Análisis exhaustivo con detalle completo de hallazgos, evidencias técnicas y pasos de corrección específicos (249€, **precio lanzamiento 179€**).
2. **Corregir riesgos críticos identificados:** Priorizar la mitigación de los hallazgos marcados como CRITICAL según las recomendaciones del Informe Técnico.
3. **Servicios adicionales disponibles:**
    - **Pack SHIELD:** Remediación técnica completa de los hallazgos detectados (360-900€ según nivel).
    - **Plan GUARDIAN:** Tranquilidad permanente con vigilancia 365×24×7 (desde 69€/mes).
    - **Fase II - Auditoría autenticada:** Análisis profundo con acceso al panel WordPress (bajo petición).

📊 ¿Necesitas más detalle?

Informe Técnico - Pack CORE (249€ | Lanzamiento 179€)

Todo lo incluido en este informe, más:

✓ Análisis exhaustivo de todos los componentes
✓ Evidencias técnicas detalladas
✓ Instrucciones de remediación paso a paso

Pack SHIELD - Remediación completa (desde 360€)

Corrección profesional de hallazgos:

✓ Corrección de todos los hallazgos detectados
✓ Implementación de mejoras técnicas
✓ Remediación delegada
✓ Informe Antes/Después con evidencias

Plan GUARDIAN - Tranquilidad permanente (desde 69€/mes)

Seguridad Gestionada y preventiva:

✓ Vigilancia y Análisis 365×24×7
✓ Detección temprana nuevos riesgos
✓ Seguridad Gestionada mensual

Tienes todo el detalle en la web de iAPentest: iapentest.com
Contacta con nosotros en: soluciones@iapentest.com

> *"Proteger un sitio web no es un gasto; es evitar que el siguiente incidente se convierta en noticia."*

Descubre todo el potencial de **iAPentest**

Características, módulos de análisis, packs disponibles y precios actualizados.

VISITA AHORA iapentest.com