Auditoría de Seguridad Web

Análisis WordPress Inteligente

[redacted]

NIVEL DE RIESGO GLOBAL

ALTO

FECHA	TIPO	ANALISTA
31/05/2026	**Informe Ejecutivo**	iAPentest

Resumen de Hallazgos

Análisis automatizado de seguridad WordPress

2	0	4	1
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: ALTO

El sitio analizado presenta un total de **7 hallazgos**: 2 críticos, 0 altos, 4 medios y 1 bajos.

💡 **¿Quieres ir más allá de este resumen?** El **Informe Técnico CORE** incluye detección completa de plugins/temas, evidencias técnicas detalladas e instrucciones de remediación paso a paso. Al final del informe encontrarás cómo agendar una llamada gratuita de 15 min para resolver tus dudas y explicarte cómo podemos ayudarte.

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 3 usuarios: [redacted], [redacted], [redacted]
2. **Protección HTTP:** Cabeceras de seguridad críticas no implementadas
3. **Protección Login:** No se detectó protección específica de login. Panel de administración expuesto a ataques de fuerza bruta.
4. **Protección WAF:** No se detectó WAF ni plugin de seguridad. Se recomienda instalar protección.
5. **Vulnerabilidades Conocidas:** Plugin(s) detectado(s) con versión no verificable: cookie-law-info. Se listan 1 vulnerabilidad(es) histórica(s) (CVE-2020-20633) que podrían NO aplicar si el plugin está actualizado. Verificar manualmente.

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. El coste medio de un ciberataque a una PYME española se sitúa entre 35.000€ y 80.000€, según INCIBE y diversos estudios del sector.
- **Disponibilidad:** Riesgo de caída del servicio por ataques. Según INCIBE, el 60% de las PYMES que sufren un ciberataque importante se ven obligadas a cerrar 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.

La puntuación de seguridad va de 0 a 100; **cuanto más cerca de 100, mejor** (100 = óptimo). El **nivel de riesgo** depende de la **gravedad** de los hallazgos detectados: un solo hallazgo crítico eleva el nivel aunque la puntuación sea intermedia.

5. Casos reales relacionados con los hallazgos (2024-2026)

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. La Conferencia Episcopal Española publica por error en su web datos de 45 víctimas de abusos.

Documento confidencial accesible públicamente durante un tiempo prolongado. Divulgación de datos especialmente sensibles sin notificación adecuada a la autoridad ni a las víctimas.

Impacto: Documento confidencial accesible públicamente durante un tiempo prolongado. Divulgación de datos especialmente sensibles sin notificación adecuada a la autoridad ni a las víctimas.

Año: 2023 | **Fuente:** El País – filtración de datos de víctimas en la web de la CEE

2. El plugin Real Estate Manager para WordPress (CVE-2023-4239) permite a usuarios con pocos permisos elevar privilegios.

Usuarios autenticados pueden modificar sus capacidades y obtener más control del sitio. Compromiso de administración de la web si una cuenta baja es explotada.

Impacto: Usuarios autenticados pueden modificar sus capacidades y obtener más control del sitio. Compromiso de administración de la web si una cuenta baja es explotada.

Año: 2023 | **Fuente:** INCIBE-CERT – CVE-2023-4239 Real Estate Manager

3. WPForms Pro para WordPress permite XSS almacenado a través de parámetros de envío (CVE-2023-7063).

Datos maliciosos enviados desde formularios pueden ejecutarse para otros usuarios. Páginas de administración o listados de envíos pueden convertirse en vector de ataque.

Impacto: Datos maliciosos enviados desde formularios pueden ejecutarse para otros usuarios. Páginas de administración o listados de envíos pueden convertirse en vector de ataque.

Año: 2024 | **Fuente:** INCIBE-CERT – CVE-2023-7063 WPForms Pro

Fuentes documentadas: Informes públicos de incidentes en WordPress, INCIBE-CERT, AEPD, estudios sectoriales de ciberseguridad, análisis de casos reales españoles 2024-2026.

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, con evidencias e instrucciones de remediación, se desarrolla en el **Informe Técnico CORE**.

Módulo	Hallazgo	Criticidad
Exposición de Usuarios	API REST expone 3 usuarios: [redacted], [redacted], [redacted]	CRÍTICO
Protección HTTP	Cabeceras de seguridad críticas no implementadas	CRÍTICO
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
Vulnerabilidades Conocidas	Plugin(s) detectado(s) con versión no verificable: cookie-law-info. Se listan 1 vulnerabilidad(es) histórica(s) (CVE-2020-20633) que podrían NO aplicar si el plugin está actualizado. Verificar manualmente.	MEDIO
Archivos Servidor	3 rutas con protección mejorable	MEDIO
Conexión Segura	HSTS no configurado. Se recomienda añadir cabecera HSTS para mayor protección	BAJO
Cumplimiento Legal	Documentación legal detectada en formato PDF. La verificación automática del contenido obligatorio (LSSI) no es posible — requiere revisión manual para confirmar presencia de NIF, titular, domicilio y email de contacto.	INFO
Exposición de Rutas	Rutas estándar de WordPress (wp-admin/wp-login) en robots.txt - informativo, sin exposición real	INFO
Certificado SSL	Certificado expira en 76 días	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
Versión PHP	PHP 8.4 con soporte activo hasta 2028-11-21	INFO
Versión WordPress	WordPress 7.0 detectado	INFO

Componentes WordPress Detectados

Se han identificado **6 plugins** y **4 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
Cookie Law Info	Plugin	N/A	⚠️ **1 CVE**
Akismet Anti-Spam	Plugin	—	⚠️ Verificar
All In One Wp Migration	Plugin	—	⚠️ Verificar
Classic Editor	Plugin	—	⚠️ Verificar
Cookie Notice	Plugin	—	⚠️ Verificar
Duplicate Page	Plugin	—	⚠️ Verificar
Divi	Tema	4.27.6	✓ OK
Twentytwentyfive	Tema	1.4	✓ OK
Twentytwentyfour	Tema	1.4	✓ OK
Twentytwentythree	Tema	1.6	✓ OK

7. Marco Normativo y Tácticas de Ataque Detectadas

Los hallazgos de esta auditoría se correlacionan con los requisitos de la **Directiva NIS2** (Directiva UE 2022/2555) y con las tácticas y técnicas del marco **MITRE ATT&CK**, estándar internacional de referencia en ciberseguridad. Esta correlación permite priorizar las acciones de remediación con criterio normativo y de inteligencia de amenazas.

Correlación con Directiva NIS2 — Artículo 21

Artículo	Requisito afectado	Valoración global
Art. 21.2.e	Seguridad en adquisición, desarrollo y mantenimiento de sistemas. **Afectado:** cabeceras HTTP de seguridad (CRÍTICO), vulnerabilidades CVE conocidas (MEDIO), firewall de aplicación web (WAF) (MEDIO). **Sin hallazgos (correcto):** versión PHP sin soporte activo, librerías JavaScript vulnerables.	CRÍTICO
Art. 21.2.i	Gestión de activos e identidades de acceso. **Afectado:** exposición de usuarios vía API REST (CRÍTICO), protección del panel de administración (MEDIO). **Sin hallazgos (correcto):** cumplimiento LSSI/RGPD.	CRÍTICO
Art. 21.2.f	Evaluación de la eficacia de las medidas de seguridad. **Afectado:** archivos y rutas sensibles expuestos (MEDIO), configuración general de WordPress (BAJO). **Sin hallazgos (correcto):** rutas expuestas en robots.txt/sitemap, exposición de versión y tecnologías, recursos externos de terceros no verificados.	MEDIO
Art. 21.2.g	Uso de criptografía y cifrado en las comunicaciones. **Sin hallazgos (correcto):** certificado TLS/HTTPS. **No aplica:** atributos de seguridad en cookies de sesión.	SIN HALLAZGOS

Correlación con MITRE ATT&CK

Técnica ID	Técnica	Táctica	Valoración global
T1562.001	Desactivación o modificación de controles de seguridad. **Afectado:** cabeceras HTTP de seguridad (CRÍTICO).	Evasión de defensas	CRÍTICO
T1589.001	Recopilación de identidades de víctimas. **Afectado:** exposición de usuarios vía API REST (CRÍTICO).	Reconocimiento	CRÍTICO

Técnica ID	Técnica	Táctica	Valoración global
T1083	Descubrimiento de archivos y directorios. **Afectado:** archivos y rutas sensibles expuestos (MEDIO), configuración general de WordPress (BAJO). **Sin hallazgos (correcto):** rutas expuestas en robots.txt/sitemap.	Descubrimiento	MEDIO
T1190	Explotación de aplicación expuesta públicamente. **Afectado:** vulnerabilidades CVE conocidas (MEDIO), firewall de aplicación web (WAF) (MEDIO). **Sin hallazgos (correcto):** versión PHP sin soporte activo.	Acceso inicial	MEDIO
T1110.001	Fuerza bruta: adivinación de contraseñas. **Afectado:** protección del panel de administración (MEDIO).	Acceso a credenciales	MEDIO
T1592	Recopilación de información del sistema objetivo. **Sin hallazgos (correcto):** cumplimiento LSSI/RGPD, exposición de versión y tecnologías.	Reconocimiento	SIN HALLAZGOS
T1557	Interceptación de comunicaciones (man-in-the-middle). **Sin hallazgos (correcto):** certificado TLS/HTTPS.	Recopilación de datos	SIN HALLAZGOS
T1195	Compromiso de la cadena de suministro. **Sin hallazgos (correcto):** recursos externos de terceros no verificados.	Acceso inicial	SIN HALLAZGOS
T1059.007	Ejecución de código JavaScript malicioso. **Sin hallazgos (correcto):** librerías JavaScript vulnerables.	Ejecución	SIN HALLAZGOS
T1539	Robo de cookies de sesión web. **No aplica:** atributos de seguridad en cookies de sesión.	Acceso a credenciales	NO APLICA

* Cada requisito agrupa varios puntos de control: **Afectado** (con hallazgo), **Sin hallazgos (correcto)** (verificado y conforme), **No aplica** (control que no procede en el sitio) y **No verificable** (aplica pero no se pudo comprobar externamente). La **Valoración global** refleja el peor hallazgo del requisito. Referencia: Directiva NIS2 (EUR-Lex) · MITRE ATT&CK (attack.mitre.org)

8. 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* *Exposición de Usuarios*
MEDIA Probabilidad	—	—	*Archivos Servidor* *Vulnerabilidades Conocidas* *Protección Login* *Protección WAF*	—
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.

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

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. **Resolver los hallazgos detectados, empezando por los críticos:** El **Informe Técnico CORE** detalla los pasos exactos para cada hallazgo.
2. **Hablar con nosotros:** Si quieres que te ayudemos a interpretar el informe, profundizar en el detalle técnico de cada hallazgo o resolver los problemas detectados, agenda una llamada gratuita. Sin compromiso.