Auditoría de Seguridad Web

Análisis WordPress Inteligente

[redacted]

NIVEL DE RIESGO GLOBAL

ALTO

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

Resumen de Hallazgos

Análisis automatizado de seguridad WordPress

2	1	3	1
CRÍTICOS	ALTOS	MEDIOS	BAJOS

1. Resumen técnico

Este análisis exhaustivo examina (con amplio detalle) todos los componentes del sitio, identificando vulnerabilidades conocidas e indicando las potenciales áreas de mejora así como su implantación.

> **Nivel de riesgo global estimado:** ALTO
>
> **Hallazgos:** 2 críticos, 1 altos, 3 medios, 1 bajos
>
> **Recomendación:** contratar **SHIELD** para la **Remediación Urgente** de los hallazgos detectados, seguido de **GUARDIAN** para la **Seguridad Gestionada**.

2. Tabla de hallazgos técnicos

Detalle técnico de los hallazgos detectados en la Fase I (análisis pasivo del perímetro público), clasificados por criticidad. Cada hallazgo incluye información sobre su impacto y prioridad de remediación.

Módulo	Hallazgo	Criticidad	OWASP
Cumplimiento Legal	Incumplimiento LSSI: El Aviso Legal no contiene datos obligatorios (NIF/CIF/NIE, Titular o Razón Social, Domicilio fiscal, Email de contacto).	CRÍTICO	–
Protección HTTP	Cabeceras de seguridad críticas no implementadas	CRÍTICO	A05:2021
JavaScript Vulnerable	Jquery 1.9.0 vulnerable a XSS (CVE-2020-11022)	ALTO	A06:2021
Protección Login	No se detectó protección específica de login. Panel de administración expuesto a ataques de fuerza bruta.	MEDIO	A07:2021
Protección WAF	No se detectó WAF ni plugin de seguridad. Se recomienda instalar protección.	MEDIO	A05:2021
Archivos Servidor	2 rutas sensibles sin protección: /wp-admin/, /wp-login.php	MEDIO	A05:2021
Conexión Segura	HSTS no configurado. Se recomienda añadir cabecera HSTS para mayor protección	BAJO	A02:2021
Versión PHP	Versión PHP no expuesta en cabeceras	INFO	A06:2021
Certificado SSL	Certificado expira en 129 días	INFO	A02:2021
Dependencias Externas	No se detectaron recursos externos	INFO	A08:2021
Ejecución PHP Directa	No se pudieron verificar plugins/themes	INFO	A05:2021
Exposición de Rutas	robots.txt y sitemap presentes, sin rutas sensibles expuestas.	INFO	A05:2021
Exposición de Usuarios	No se detectaron usuarios enumerables. El sitio no expone información de autores públicamente.	INFO	A01:2021
Plugins de Riesgo	No se detectaron plugins en HTML público.	INFO	A06:2021
Versión WordPress	Servidor web Apache identificado	INFO	A06:2021

Módulo	Hallazgo	Criticidad	OWASP
Vulnerabilidades Conocidas	No se detectaron vulnerabilidades conocidas con CVE en plugins o temas	INFO	A06:2021

ℹ️ Clasificación OWASP Top 10

Los hallazgos se correlacionan con el estándar **OWASP Top 10:2021**, referencia internacional para identificar riesgos en aplicaciones web. Este estándar es utilizado por frameworks de cumplimiento como PCI DSS e ISO 27001.

Fuente: owasp.org/Top10/2021/

3. 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), librerías JavaScript vulnerables (ALTO), firewall de aplicación web (WAF) (MEDIO), plugins desactualizados (BAJO). **Sin hallazgos (correcto):** versión PHP sin soporte activo, vulnerabilidades CVE conocidas.	CRÍTICO
Art. 21.2.i	Gestión de activos e identidades de acceso. **Afectado:** cumplimiento LSSI/RGPD (CRÍTICO), protección del panel de administración (MEDIO), exposición de usuarios vía API REST (BAJO).	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	Evidencia detectada	Valoración global
T1562.001	Desactivación o modificación de controles de seguridad. **Afectado:** cabeceras HTTP de seguridad (CRÍTICO).	Evasión de defensas	Faltan cabeceras críticas como content-security-policy, strict-transport-security; se recomienda revisión prioritaria.	CRÍTICO

Técnica ID	Técnica	Táctica	Evidencia detectada	Valoración global
T1592	Recopilación de información del sistema objetivo. **Afectado:** cumplimiento LSSI/RGPD (CRÍTICO). **Sin hallazgos (correcto):** exposición de versión y tecnologías.	Reconocimiento	Incumplimiento LSSI: El Aviso Legal no contiene datos obligatorios (NIF/CIF/NIE, Titular o Razón Social, Domicilio fiscal, Email de contacto). Riesgo de sanción.	CRÍTICO
T1059.007	Ejecución de código JavaScript malicioso. **Afectado:** librerías JavaScript vulnerables (ALTO).	Ejecución	Jquery 1.9.0 vulnerable a XSS (CVE-2020-11022)	ALTO
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	2 rutas sensibles sin protección: /wp-admin/, /wp-login.php	MEDIO
T1110.001	Fuerza bruta: adivinación de contraseñas. **Afectado:** protección del panel de administración (MEDIO).	Acceso a credenciales	No se detectó protección específica de login. Panel de administración expuesto a ataques de fuerza bruta.	MEDIO

Técnica ID	Técnica	Táctica	Evidencia detectada	Valoración global
T1190	Explotación de aplicación expuesta públicamente. **Afectado:** firewall de aplicación web (WAF) (MEDIO), plugins desactualizados (BAJO). **Sin hallazgos (correcto):** versión PHP sin soporte activo, vulnerabilidades CVE conocidas.	Acceso inicial	No se detectó WAF ni plugin de seguridad. Se recomienda instalar protección.	MEDIO
T1589.001	Recopilación de identidades de víctimas. **Afectado:** exposición de usuarios vía API REST (BAJO).	Reconocimiento	No se detectaron usuarios enumerables. El sitio no expone información de autores públicamente.	BAJO
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

Técnica ID	Técnica	Táctica	Evidencia detectada	Valoración global
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)

4. Instrucciones de remediación

A continuación se detallan las instrucciones técnicas para corregir cada hallazgo, ordenadas por criticidad.

1. Cumplimiento Legal CRÍTICO

Acción: Verificar y completar páginas legales obligatorias

Dónde: Páginas WordPress + enlaces visibles en footer/menú

Pasos a seguir:

- Implementar banner de cookies con opción de rechazo (Complianz, CookieYes)
- Crear páginas legales (Política de Privacidad, Aviso Legal, Cookies)
- Añadir enlaces a páginas legales en footer o menú principal

Ejemplo:

```
Ubicar enlaces legales en footer para cumplir con requisitos de accesibilidad RGPD
```

2. Protección HTTP CRÍTICO

Acción: Implementar cabeceras de seguridad HTTP

Dónde: Archivo .htaccess en la raíz del sitio o configuración del servidor

Pasos a seguir:

- X-Frame-Options: DENY (previene clickjacking)
- X-Content-Type-Options: nosniff (evita MIME sniffing)
- X-XSS-Protection: 1; mode=block (protección XSS navegador)
- Referrer-Policy: strict-origin-when-cross-origin
- Permissions-Policy: geolocation=(), microphone=(), camera=()
- Content-Security-Policy: default-src 'self' (ajustar según necesidades)

Ejemplo:

```
Header always set X-Frame-Options "DENY"
Header always set X-Content-Type-Options "nosniff"
```

3. JavaScript Vulnerable ALTO

Acción: Actualizar bibliotecas JavaScript vulnerables

Dónde: Archivos JavaScript del tema y plugins de WordPress

Pasos a seguir:

- Actualizar WordPress a la última versión (incluye jQuery actualizado)
- Actualizar el tema activo a su última versión
- Actualizar todos los plugins que incluyan bibliotecas JavaScript
- Si el tema o plugin no tiene actualizaciones, considerar alternativas
- Verificar que no haya bibliotecas JS cargadas manualmente en el tema hijo

Ejemplo:

```
Para verificar versión de jQuery en consola del navegador:
jQuery.fn.jquery

Versiones seguras mínimas:
- jQuery: 3.5.0+
- jQuery UI: 1.13.0+
- Lodash: 4.17.21+
```

4. Protección Login MEDIO

Acción: Proteger acceso al panel de administración

Dónde: Panel de administración WordPress > Plugins y configuración

Pasos a seguir:

- Instalar plugin de limitación de intentos (Limit Login Attempts Reloaded)
- Considerar implementar autenticación de dos factores (2FA)
- Opcionalmente ocultar URL de login con WPS Hide Login
- Usar contraseñas fuertes y únicas para todos los usuarios
- Limitar usuarios con rol de administrador al mínimo necesario
- Revisar y eliminar usuarios inactivos o sospechosos

Ejemplo:

```
Plugins recomendados:
- Limit Login Attempts Reloaded (bloqueo de IPs)
- WP 2FA o Google Authenticator (2FA)
- WPS Hide Login (ocultar wp-login.php)
- Loginizer (protección completa)
```

5. Protección WAF MEDIO

Acción: Instalar plugin de seguridad WAF

Dónde: Panel de administración WordPress > Plugins

Pasos a seguir:

- Instalar un plugin de seguridad como Wordfence, Sucuri o All In One WP Security
- Configurar el firewall de aplicaciones web (WAF) del plugin
- Activar protección contra fuerza bruta en login
- Habilitar escaneo de malware periódico
- Configurar alertas de seguridad por email
- Considerar Cloudflare como capa adicional de protección

Ejemplo:

```
Plugins recomendados (gratuitos):
- Wordfence Security (más popular, WAF completo)
- Sucuri Security (escaneo de malware)
- All In One WP Security (fácil de usar)
- iThemes Security (protección login)
```

6. Archivos Servidor MEDIO

Acción: Configurar protecciones en .htaccess

Dónde: Archivo .htaccess en la raíz del sitio WordPress

Pasos a seguir:

- Proteger archivos sensibles (.htaccess, wp-config.php, etc.)
- Bloquear acceso a archivos de log y backup
- Prevenir ejecución de PHP en /uploads/
- Bloquear bots maliciosos conocidos
- Configurar protección contra hotlinking de imágenes

Ejemplo:

```
Bloquear PHP en uploads:
<Directory /wp-content/uploads/>
<Files *.php>
Deny from all
</Files>
</Directory>
```

5. Alcance y metodología

Alcance de la auditoría

- **Tipo:** Análisis pasivo y no intrusivo desde perímetro público (Fase I)
- **Metodología:** Recopilación automatizada de señales técnicas visibles sin autenticación, con análisis asistido por IA
- **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 del análisis

- Este análisis refleja el estado del sitio en el momento de la auditoría
- Vulnerabilidades internas o con acceso autenticado requieren Fase II
- El análisis pasivo puede no detectar todos los componentes instalados
- Plugins premium o personalizados pueden no ser identificados completamente

📊 ¿Necesitas ayuda con la remediación?

Las instrucciones de remediación de este informe te permiten corregir cada hallazgo, siempre que cuentes con unos conocimientos técnicos mínimos de WordPress. Si prefieres delegarlo, podemos encargarnos nosotros; estas son tus opciones:

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

Fase II - Auditoría autenticada

Análisis profundo con acceso al panel WordPress (bajo petición).

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