Auditoría de Seguridad Web

Análisis WordPress Inteligente

test-url.com

NIVEL DE RIESGO GLOBAL

CRÍTICO

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

Resumen de Hallazgos

Análisis automatizado de seguridad WordPress

4	1	4	0
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:** CRÍTICO
>
> **Hallazgos:** 4 críticos, 1 altos, 4 medios, 0 bajos
>
> **Recomendación:** Se recomienda contratar el servicio **SHIELD** para remediación urgente de los hallazgos críticos, seguido de **GUARDIAN** para 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
Exposición de Usuarios	API REST expone 2 usuarios: `admin_webmaster`, `javier_marketing`	CRÍTICO	A01:2021
Versión PHP	PHP 7.4 sin soporte desde 2022-11-28. PHP sin soporte activo	CRÍTICO	A06:2021
Vulnerabilidades Conocidas	Detectada(s) 11 vulnerabilidad(es) en componentes instalados (CVE-2022-2267, CVE-2022-2556, CVE-2024-39666)	CRÍTICO	A06:2021
Protección HTTP	Cabeceras de seguridad críticas no implementadas	CRÍTICO	A05:2021
Versión WordPress	WordPress 6.5.7 desactualizado (actual: 6.9)	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
Exposición de Rutas	Rutas administrativas estándar expuestas en robots.txt.	MEDIO	A05:2021
Archivos Servidor	3 rutas sensibles sin protección: /wp-admin/install.php, /wp-content/plugins/, /wp-content/themes/	MEDIO	A05:2021
Cumplimiento Legal	Cumplimiento legal correcto. Páginas legales completas con elementos obligatorios RGPD/LOPDGDD.	INFO	—
Plugins Problemáticos	Ningún plugin clasificado como crítico para rendimiento	INFO	A06:2021
Certificado SSL	Certificado expira en 31 días	INFO	A02:2021
Conexión Segura	Conexión segura correctamente configurada (HTTPS + HSTS)	INFO	A02:2021
Dependencias Externas	No se detectaron recursos externos	INFO	A08:2021

Módulo	Hallazgo	Criticidad	OWASP
Ejecución PHP Directa	Ejecución de código PHP correctamente bloqueada en rutas de plugins	INFO	A05:2021
JavaScript Vulnerable	Todas las bibliotecas JavaScript detectadas (2) están actualizadas	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/

Componentes WordPress Detectados

Se han identificado **12 plugins** y **3 temas** mediante análisis exhaustivo externo.

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

Componente	Tipo	Versión	Estado
Test Url Theme	Tema	4.26.0	✓ OK

3. Instrucciones de remediación

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

1. Exposición de Usuarios CRÍTICO

Acción: Bloquear enumeración de usuarios

Dónde: Archivo functions.php del tema hijo o plugin de seguridad

Pasos a seguir:

- Bloquear acceso a ?author=N en .htaccess
- Deshabilitar endpoint REST API de usuarios
- No usar 'admin' como nombre de usuario
- Configurar slug de autor diferente al username
- Usar plugin de seguridad (Wordfence, iThemes Security)

Ejemplo:

```
En .htaccess:
RewriteCond %{QUERY_STRING} ^author=
RewriteRule .* - [F,L]
```

2. Versión PHP CRÍTICO

Acción: Actualizar versión de PHP

Dónde: Panel de hosting (cPanel, Plesk) o contactar con proveedor

Pasos a seguir:

- Verificar compatibilidad de plugins/tema con PHP 8.x
- Hacer backup completo antes de actualizar
- Cambiar versión PHP en el panel de hosting
- Probar el sitio exhaustivamente tras el cambio
- Versiones recomendadas: PHP 8.1 o superior

Ejemplo:

```
En cPanel: Select PHP Version > Cambiar a PHP 8.1 o 8.2
```

3. Vulnerabilidades Conocidas CRÍTICO

Acción: Corregir vulnerabilidades conocidas (CVE)

Dónde: Panel wp-admin > Plugins/Temas y configuración del servidor

Pasos a seguir:

- Actualizar plugins/temas con CVEs conocidos inmediatamente
- Si no hay actualización disponible, desactivar el plugin vulnerable
- Buscar alternativas para plugins abandonados con vulnerabilidades
- Revisar changelog de actualizaciones para confirmar parches de seguridad
- Monitorizar nuevas vulnerabilidades en bases de datos públicas de seguridad

Ejemplo:

```
Consultar CVEs en: https://nvd.nist.gov/vuln/search o https://patchstack.com/database/
```

4. 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"
```

5. Versión WordPress ALTO

Acción: Actualizar WordPress y ocultar versión

Dónde: Panel de administración wp-admin y functions.php

Pasos a seguir:

- Actualizar WordPress desde Escritorio > Actualizaciones
- Hacer backup completo antes de actualizar
- Ocultar versión WP: remove_action('wp_head', 'wp_generator');
- Eliminar archivo readme.html de la raíz
- Mantener actualizaciones automáticas de seguridad activas

Ejemplo:

```
En functions.php:
remove_action('wp_head', 'wp_generator');
```

6. 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)
```

7. 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)
```

8. Exposición de Rutas MEDIO

Acción: Minimizar información en robots.txt y sitemap

Dónde: Archivo robots.txt en la raíz y configuración de plugin SEO

Pasos a seguir:

- No revelar rutas sensibles en robots.txt (Disallow)
- Eliminar referencias a wp-admin, wp-includes si las hay
- Verificar que sitemap no exponga URLs privadas
- Configurar correctamente plugin SEO (Yoast, Rank Math)
- Revisar que no haya backups o archivos sensibles indexados

Ejemplo:

```
robots.txt mínimo:
User-agent: *
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php
Sitemap: https://tusitio.com/sitemap.xml
```

9. 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>
```

4. 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 del sitio

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?

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

> *"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

TODOS LOS PRECIOS AQUÍ INDICADOS SON MÁS IVA (21%)