EXOLOGIC SYSTEMS

Reporte de Seguridad WordPress

https://brainy-competition.localsite.io/

Tu sitio presenta riesgos altos. Actuar pronto reduce significativamente tu exposición.

Alto Riesgo

Análisis realizado el 14 de mayo de 2026, 09:33 CST

Resumen Ejecutivo

0	1	6	0
CRÍTICO	ALTO	MEDIO	BAJO

Top 3 Hallazgos Más Urgentes

1. **Contact Form 7 <= 5.3.1 - Arbitrary File Upload via Bypass**
   Contact Form 7 — ALTO

2. **Contact Form 7 <= 5.9 - Reflected Cross-Site Scripting**
   Contact Form 7 — MEDIO

3 **Contact Form 7 <= 5.9.4 - Unauthenticated Open Redirect**
Contact Form 7 — MEDIO

Limitaciones del análisis: Este reporte es el resultado de un análisis externo de superficie pública. ExoScan WP no accede al servidor del sitio ni a su base de datos interna. Los hallazgos marcados como "Probable" son inferidos y pueden no aplicar si el sitio usa configuraciones no estándar. Un score alto no garantiza ausencia total de vulnerabilidades desconocidas.

Vulnerabilidades Detectadas (7)

ALTO Confianza: Estimado — podría variar CVSS: 8.1

Contact Form 7 <= 5.3.1 - Arbitrary File Upload via Bypass

Componente: **Contact Form 7** — Versiones afectadas: Todas las versiones hasta 5.3.2 CVE-2020-35489

Un delincuente informático puede usar el formulario de contacto de tu sitio para subir archivos maliciosos que le den acceso total a tu página web, como si tuviera las llaves de tu tienda. Con esto puede robar información de tus clientes, datos bancarios, modificar tu sitio para engañar a la gente, o dejar tu negocio offline sin poder vender. Debes actualizar el plugin "Contact Form 7" a la versión 5.3.2 o superior ahora mismo, sin esperar. Si no sabes hacerlo, contacta a tu proveedor de hosting o a un técnico que te ayude porque cada hora que pase tu negocio está expuesto a un ataque real.

Requiere autenticación	**No**	Versión con parche	**5.3.2**

MEDIO Confianza: Estimado — podría variar CVSS: 6.1

Contact Form 7 <= 5.9 - Reflected Cross-Site Scripting

Componente: **Contact Form 7** — Versiones afectadas: Todas las versiones hasta 5.9 CVE-2024-2242

El formulario de contacto de tu sitio web tiene una vulnerabilidad que permite a un atacante insertar código malicioso que se ejecuta en el navegador de tus visitantes. Si alguien aprovecha esto, podría robar información de tus clientes, como sus datos de contacto o contraseñas, o engañarlos para que descarguen virus. Lo que debes hacer es muy simple: actualiza el plugin Contact Form 7 a la versión 5.10 o más nueva lo antes posible. Si necesitas ayuda, contacta a tu proveedor de hosting o a un profesional de informática, pero no esperes mucho tiempo para hacerlo.

Requiere autenticación	**No**	Versión con parche	**5.9.2**

MEDIO Confianza: Estimado — podría variar

CVSS: 6.1

Contact Form 7 <= 5.9.4 - Unauthenticated Open Redirect

Componente: **Contact Form 7** — Versiones afectadas: Todas las versiones hasta 5.9.4 CVE-2024-4704

El plugin Contact Form 7 tiene un error que permite a los atacantes insertar enlaces falsos en tus formularios de contacto, de modo que cuando tus clientes hacen clic, son redirigidos a sitios maliciosos sin que se note. Es como si alguien modificara discretamente las direcciones en tus tarjetas de presentación para enviar a la gente a lugares que no son. Si un atacante aprovecha esto, tus clientes podrían terminar en sitios de phishing donde pierden dinero o datos bancarios, y ellos te culparán a ti por la estafa. Además, tu reputación se daña porque la gente verá tu negocio como poco confiable o comprometido, lo que te hace perder ventas y clientes a largo plazo. Entra en tu panel de WordPress, ve a Plugins, busca Contact Form 7, y asegúrate de que está actualizado a la versión 5.9.5 o superior. Si aparece un botón que dice Actualizar, haz clic inmediatamente. Después verifica que tus formularios de contacto sigan funcionando bien enviándote un mensaje de prueba a ti mismo.

Requiere autenticación	**No**	Versión con parche	**5.9.5**

MEDIO Confianza: Estimado — podría variar

CVSS: 5.3

WordPress Core - All Known Versions - Cleartext Storage of wp_signups.activation_key

Componente: **WordPress** — Versiones afectadas: Todas las versiones hasta * CVE-2017-14990

WordPress guarda las claves de activación de nuevas cuentas de usuarios en texto plano, sin encriptar. Esto significa que cualquiera que logre acceder a tu base de datos puede ver esas claves y usarlas para crear cuentas falsas o acceder a perfiles que aún no están completamente activados, como si fuera el usuario legítimo. Si un atacante explota esto, puede crear cuentas administrativas en tu sitio sin tu permiso, robar información de clientes que se registraron, o modificar contenido y productos de tu tienda online. También podría usar tu sitio para enviar estafas a tus clientes, destruyendo la confianza que construiste y afectando tus ventas. Lo primero es mantener WordPress actualizado a la versión más reciente, ya que esto incluye correcciones de seguridad. También debes usar un plugin de seguridad confiable que proteja tu base de datos, cambiar las contraseñas de acceso a tu servidor y base de datos, y si es posible, limitar quién puede acceder a tu panel de WordPress usando una dirección IP específica. Revisa regularmente qué cuentas de usuario existen en tu sitio y elimina las que no reconozcas.

Requiere autenticación	**No**	Versión con parche	**Ver changelog del plugin**

MEDIO Confianza: Estimado — podría variar

CVSS: 5.3

Contact Form 7 <= 6.0.5 - Order Replay Vulnerability

Componente: **Contact Form 7** — Versiones afectadas: Todas las versiones hasta 6.0.5 CVE-2025-3247

Imagina que tu formulario de contacto es como una puerta de tu tienda física. Contact Form 7 tiene una falla que permite a alguien repetir o "reproducir" acciones que clientes anteriores ya realizaron, como si grabara cada movimiento y lo pudiera tocar de nuevo. Un atacante puede capturar el formulario que envió un cliente hace días y reenviarlo múltiples veces sin que sea necesario llenar nada de nuevo, usando exactamente los mismos datos. Esta vulnerabilidad puede generar caos en tu negocio porque alguien podría enviar órdenes falsas, registros duplicados o mensajes de spam masivo usando tus formularios legítimos. Si vendes por internet o recolectas datos de clientes, podrías recibir decenas de pedidos fantasma, confirmar compras que nunca existieron, o contaminar tu base de datos con información repetida que te haga perder tiempo valioso limpiando registros. Además, afecta la confianza de tus clientes reales al ver que sus datos pueden ser manipulados así. Entra a tu panel de WordPress, ve a Plugins y busca Contact Form 7 en la lista instalada. Si tienes una versión igual o anterior a la 6.0.5, haz clic inmediatamente en el botón Actualizar que aparecerá en ese plugin. Espera a que termine la actualización, que generalmente toma segundos. Luego verifica que tus formularios de contacto sigan funcionando correctamente probándolos tú mismo con un mensaje de prueba. Si usas versiones posteriores a la 6.0.5 ya estás protegido, pero es buena idea revisar ahora mismo para estar seguro.

Requiere autenticación	**No**	Versión con parche	**6.0.6**

MEDIO Confianza: Estimado — podría variar

CVSS: 4.0

WordPress Core - All known versions - Unauthenticated Blind Server Side Request Forgery

Componente: **WordPress** — Versiones afectadas: Todas las versiones hasta * CVE-2022-3590

Un atacante puede engañar a tu servidor de WordPress para que haga peticiones a otros sitios o sistemas internos sin que tú lo autorices, como si fuera una orden legítima que viene de tu propio negocio. Es como si alguien usara tu teléfono para hacer llamadas sin que tú lo sepas. Si alguien aprovecha esto, podría acceder a información privada de tu negocio, robar datos de clientes, o usar tu servidor para atacar otros sitios y dejarte a ti como responsable. También podría interferir con sistemas que tiene tu empresa conectados a internet, causando que dejes de poder acceder a tus propios datos. Debes actualizar WordPress a la última versión disponible lo antes posible, ya que los desarrolladores han corregido este fallo. Entra a tu panel de administración, ve a Actualizaciones y aplica cualquier actualización de WordPress Core que veas disponible. Si tu sitio tiene plugins que no actualizan automáticamente, también revisa que todos estén en su versión más reciente.

Requiere autenticación	**No**	Versión con parche	**Ver changelog del plugin**

MEDIO Confianza: Estimado — podría variar CVSS: 6.6

Contact Form 7 <= 5.8.3 - Authenticated (Editor+) Arbitrary File Upload

Componente: **Contact Form 7** — Versiones afectadas: Todas las versiones hasta 5.8.3 CVE-2023-6449

El plugin Contact Form 7 que usas para que tus clientes te envíen mensajes tiene un agujero de seguridad que permite a personas que tengan acceso a tu panel de WordPress (empleados, colaboradores o alguien que haya robado una contraseña) subir archivos maliciosos a tu servidor sin que lo notes. Si alguien aprovecha esto, podría insertar virus en tu sitio web, robar información de tus clientes, hacer que tu negocio aparezca como no confiable ante Google, o usar tu servidor para atacar a otras personas, lo que te traería problemas legales y destruiría la confianza que tus clientes tienen en ti. Entra a tu panel de WordPress, ve a Plugins, busca Contact Form 7 y actualiza el plugin a la versión más reciente haciendo clic en el botón de actualizar, luego cambia las contraseñas de todos los usuarios que tengan acceso a tu panel de administración para asegurarte de que nadie no autorizado pueda entrar.

Requiere autenticación	**Sí (Editor+)**	Versión con parche	**5.8.4**

Componentes Detectados

Componente	Versión	Confianza
WordPress Core	6.9.4	Detectado con certeza
Woocommerce (plugin)	10.6.1	Estimado — podría variar
Contact Form 7 (plugin)	5.3.1	Estimado — podría variar
Twenty Twenty-Five (theme)	1.4	Detectado con certeza

Configuración de Seguridad

Headers HTTP

X-Frame-Options	✗ Ausente
X-Content-Type-Options	✗ Ausente
Content-Security-Policy	✗ Ausente
Strict-Transport-Security	✗ Ausente

Referrer-Policy	✗ Ausente
Permissions-Policy	✗ Ausente

Estos encabezados son configuraciones técnicas del servidor web. Su activación depende de tu proveedor de hosting, no de WordPress directamente. Comparte este reporte con tu proveedor de confianza para que los active — la mayoría los habilita sin costo adicional.

Configuraciones WordPress y SSL

xmlrpc.php expuesto	✓ OK
Enumeración usuarios (/?author=1)	✓ OK
Enumeración usuarios (REST API)	✗ Inseguro
Debug log expuesto	✓ OK
Directory listing en /plugins/	✓ OK
Directory listing en /themes/	✓ OK
wp-config.php accesible	✓ OK
readme.html accesible	✗ Inseguro
Certificado SSL/TLS	✓ Válido
Redirect HTTP → HTTPS	✓ Activo

Los ítems marcados como Inseguro son configuraciones que puedes corregir desde tu panel de administración de WordPress o con ayuda de tu desarrollador. No requieren acceso al servidor.

Sobre Este Análisis

Este reporte fue generado por **ExoScan WP**, un scanner de seguridad externo desarrollado por ExoLogic Systems. El análisis se realiza exclusivamente sobre la superficie pública del sitio — información visible en respuestas HTTP, HTML, headers y archivos estáticos.

Fuentes de datos: Wordfence Intelligence como fuente primaria de vulnerabilidades WordPress.

Nota legal: Este análisis es solo informativo. ExoLogic Systems no se responsabiliza por decisiones tomadas basándose únicamente en este reporte. Se recomienda complementar con una auditoría de seguridad profesional para sistemas críticos.

Generated by ExoScan WP — ExoLogic Systems

14 de mayo de 2026, 09:33 CST

Este reporte contiene información de seguridad confidencial de tu sitio. Compártelo únicamente con tu proveedor de hosting o desarrollador de confianza para corregir los puntos detectados.