EXOLOGIC SYSTEMS

WordPress Security Report

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

Alto Riesgo

Análisis realizado el 25 de marzo de 2026, 00:12 UTC
Tier: Básico · Duración: 52.9s

Resumen Ejecutivo

0	2	7	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. **WordPress Core 5.8 beta - Stored Cross-Site Scripting in Custom HTML Block**
   WordPress — ALTO

3. **WordPress Core 5.8 beta - Block Editor Authorization Bypass**
   WordPress — 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 (9)

ALTO Confianza: Probable

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**

RECOMENDACIÓN

Actualizar Contact Form 7 a la versión 5.3.2 o superior.

ALTO Confianza: Probable CVSS: 7.6

WordPress Core 5.8 beta - Stored Cross-Site Scripting in Custom HTML Block

Componente: **WordPress** — Versiones afectadas: 5.8 beta 1 - 5.8 beta 2 CVE-2021-39202

La vulnerabilidad que tienen es como dejar una puerta abierta en su sitio web que permite a delincuentes inyectar código malicioso que afecta a todos sus visitantes. Esto significa que los clientes que entren a su página podrían ser redirigidos a sitios fraudulentos, sus datos personales o de tarjeta podrían ser robados, o su reputación dañada si ven contenido extraño o peligroso en su sitio. Lo que deben hacer ahora mismo es actualizar WordPress a la versión más reciente disponible, cambiar todas las contraseñas de administrador y revisar si alguien no autorizado ha accedido a su panel de control recientemente. Si no saben cómo hacerlo, contacten a su proveedor de hosting o a un técnico especializado para que lo haga sin demora, porque cada momento que pase el riesgo de que alguien malintencionado explote esta puerta abierta es más grande.

Requiere autenticación	**No**	Versión con parche	**5.8**

RECOMENDACIÓN

Actualizar WordPress a la versión 5.8 o superior.

MEDIO Confianza: Probable CVSS: 6.8

WordPress Core 5.8 beta - Block Editor Authorization Bypass

Componente: **WordPress** — Versiones afectadas: 5.8 beta 1 - 5.8 beta 1 CVE-2021-39203

QUE ES: Es un problema de seguridad encontrado en una versión de prueba de WordPress donde alguien sin permisos suficientes podría acceder y modificar contenido del sitio que en teoría no debería poder tocar. QUE RIESGO REPRESENTA: Si un empleado poco confiable o un atacante logra entrar al sitio, podría cambiar o eliminar información importante, publicar mensajes falsos con su nombre de empresa, o dejar el sitio inutilizable sin que usted lo autorices. QUE HACER: Actualice WordPress a la versión más reciente disponible en su panel de administración, revise quiénes tienen acceso a su sitio y asegúrese de que solo personal de confianza tenga permisos para editar contenido.

Requiere autenticación	**No**	Versión con parche	**5.8**

RECOMENDACIÓN

Actualizar WordPress a la versión 5.8 o superior.

MEDIO Confianza: Probable 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

QUE ES Tu sitio web usa un complemento llamado Contact Form 7 para que los visitantes te envíen mensajes. En las versiones antiguas de este complemento existe un problema de seguridad que permite a ciertos usuarios autorizados en tu sitio subir archivos maliciosos sin que el sistema lo evite. RIESGO PARA TU NEGOCIO Si alguien aprovecha este fallo, podría subir un archivo dañino que afecte el funcionamiento de tu sitio web, robe información de tus clientes, o tome el control de tu página completa. Esto significaría pérdida de confianza de tus clientes, posible robo de datos personales, y daños graves a tu reputación. QUE DEBES HACER Necesitas actualizar inmediatamente el complemento Contact Form 7 a una versión más nueva que cierre este problema. Accede a tu panel de administración del sitio web, busca la sección de complementos, y haz clic en actualizar cuando veas disponible la nueva versión.

Requiere autenticación	**No**	Versión con parche	**5.8.4**

RECOMENDACIÓN

Actualizar Contact Form 7 a la versión 5.8.4 o superior.

MEDIO Confianza: Probable 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

QUÉ ES El plugin Contact Form 7 que usa tu sitio web tiene un problema de seguridad. Los atacantes pueden hacer que el formulario de contacto redirija a los visitantes hacia sitios falsos o peligrosos sin que se note que es una trampa. RIESGO PARA TU NEGOCIO Si alguien usa este defecto, puede engañar a tus clientes haciéndoles creer que están en tu sitio cuando en realidad están en uno falso. Así pueden robar datos de tus clientes, dinero, o infecciones de virus, y todo quedará asociado con tu negocio, dañando tu reputación. QUÉ DEBES HACER Actualiza el plugin Contact Form 7 a una versión más nueva que 5.9.4 lo antes posible. Solo entra al panel de administración de tu sitio, ve a plugins y busca la opción de actualizar. Si no sabes cómo hacerlo, pídele ayuda a tu proveedor de hosting o a un técnico de confianza.

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

RECOMENDACIÓN

Actualizar Contact Form 7 a la versión 5.9.5 o superior.

MEDIO Confianza: Probable

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**

RECOMENDACIÓN

Actualizar Contact Form 7 a la versión 5.9.2 o superior.

MEDIO Confianza: Probable

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 el código de activación de cuentas nuevas de usuarios en texto plano, sin encriptación. Esto significa que alguien con acceso a la base de datos de tu sitio podría ver estos códigos y crear cuentas falsas o tomar control de registros de usuarios nuevos. El riesgo para tu negocio es que un atacante podría registrarse con cuentas fraudulentas, acceder a información de clientes, publicar contenido malicioso en tu sitio, o enviar correos de spam desde tu dominio dañando tu reputación. Para prevenirlo debes actualizar WordPress a la última versión disponible, mantener un respaldo seguro de tu base de datos, y usar complementos de seguridad que protejan el acceso a tu información sensible. Si tu sitio permite registros de usuarios, revisa quién se ha registrado recientemente para detectar cuentas sospechosas.

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

RECOMENDACIÓN

Actualizar WordPress a la última versión disponible.

MEDIO Confianza: Probable 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

QUE ES El formulario de contacto de tu sitio web tiene un problema de seguridad. Los atacantes pueden repetir o modificar las acciones que los clientes legítimos envían a través de este formulario sin que el sistema lo detecte. RIESGO PARA TU NEGOCIO Si alguien explota esto podría enviar múltiples pedidos falsos usando los datos de tus clientes reales, generar cargos duplicados en tarjetas de crédito, o causar confusión con información ficticia que parece venir de personas de verdad. Esto daña la confianza de tus clientes y tu reputación. QUE DEBES HACER Actualiza el plugin Contact Form 7 a la versión más reciente disponible en tu sitio web. Es una tarea simple que normalmente toma pocos minutos y soluciona automáticamente el problema de seguridad.

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

RECOMENDACIÓN

Actualizar Contact Form 7 a la versión 6.0.6 o superior.

MEDIO Confianza: Probable 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

Qué es: Un atacante puede obligar a tu sitio web de WordPress a hacer acciones sin que nadie lo autorice, como si fuera un cliente más visitando tu página. Riesgo para el negocio: Si alguien explota esto, podría usar tu sitio como intermediario para atacar otros sistemas, robar información sobre tu red interna, o hacer que tu página se vea comprometida, lo que afecta la confianza de tus clientes. Qué debes hacer: Mantén WordPress siempre actualizado a la última versión disponible, asegúrate de que tu proveedor de hosting tenga buenas medidas de seguridad, y considera contratar a alguien que revise regularmente la salud de tu sitio web.

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

RECOMENDACIÓN

Actualizar WordPress a la última versión disponible.

Componentes Detectados

Componente	Versión	Confianza
WordPress Core	6.9.4	Confirmado
Woocommerce (plugin)	10.6.1	Probable
Contact Form 7 (plugin)	5.3.1	Probable
Twenty Twenty-Five (theme)	1.4	Confirmado

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.