swpanel

ANÁLISIS DE CÓDIGO Y CORRECCIÓN AUTOMÁTICA · PREMIUM

Auditoría de errores y correcciones

Detección y reparación de errores de programación a partir de los logs de Apache/Nginx.

Tiempo de análisis: 6m 28s

DOMINIO	ERRORES DETECTADOS	FICHEROS AFECTADOS
swpanel.com (DEMO)	5 (2 críticos)	4
CORRECCIONES	**FECHA**	**DOCUMENTO**
4 / 4	16/10/2026	SW-COD-EJEMPLO-2026

Se analizan los registros (logs) del 05-10-2026 al 12-10-2026

ÍNDICE

Índice

01 Resumen ejecutivo de seguridad **2**

02 Resumen del análisis **6**

Introducción 7
Resumen ejecutivo 8
Errores detectados 9

03 Seguridad y detección de malware **10**

Cómo funciona este análisis 11
template-tags.php 12
functions.php 13
class-pricing.php 14
export.php 15

04 Correcciones propuestas **16**

template-tags.php 17
functions.php 19
class-pricing.php 21
export.php 23

05 Errores SQL detectados **25**

06 Diagnóstico del tráfico **27**

07 Tráfico y seguridad (logs de acceso) **31**

08 Errores de JavaScript **35**

Cómo funciona este análisis 36

09 Estado del CMS **38**

10 Versión y soporte de PHP **45**

11 Integridad del núcleo de WordPress **47**

12 Exposición y superficie de ataque **49**

13 Directivas maliciosas de configuración **51**

14 Ataques detectados en los registros **53**

15 Tráfico e indicadores de red maliciosos **58**

16 Matriz de Impacto en Negocio **61**

17 Conclusiones **63**

Glosario de términos **67**

Análisis de SWPANEL.COM generado por SWPanel

01

Resumen ejecutivo de seguridad

Visión de conjunto del estado de seguridad del sitio y las prioridades de actuación.

Análisis de SWPANEL.COM generado por SWPanel

Resumen ejecutivo de seguridad

Visión de conjunto del estado de seguridad del sitio y las prioridades de actuación.

PUNTUACIÓN DE RIESGO

72 / 100

Riesgo ALTO

ACTIVIDAD DE ATAQUE Y VULNERABILIDADES

9	Ataques contra vulnerabilidades reales de la web
386	Intentos de ataque en los registros
2	Vulnerabilidades conocidas (CVE)
3	IPs maliciosas que han accedido
5	Errores de código

El estado general de seguridad del sitio web se encuentra en un nivel alto de riesgo, con una puntuación de 72 sobre 100. Esta valoración refleja principalmente la cantidad de intentos de ataque registrados, junto con la presencia de algunas vulnerabilidades que, aunque no están actualmente siendo explotadas, podrían ser aprovechadas en el futuro si no se abordan. Afortunadamente, no se han encontrado archivos con código malicioso en el disco ni conexiones con servidores de control remoto, lo que sugiere que no hay evidencia de un compromiso activo en este momento. Sin embargo, la situación requiere atención inmediata para evitar que se convierta en algo más grave.

Los registros muestran que el sistema ha sido atacado en 386 ocasiones, de las cuales 9 han sido dirigidas a vulnerabilidades reales del software. Aunque estos intentos no han tenido éxito hasta ahora, indican que hay actores maliciosos que están buscando aprovechar puntos débiles. Las IPs con reputación maliciosa detectadas y las vulnerabilidades identificadas representan una amenaza real, ya que pueden facilitar el acceso no autorizado si no se resuelven. Por otro lado, el hecho de que no haya señales de código malicioso ni comunicación con servidores de control es un factor tranquilizador, ya que sugiere que el sistema no ha sido comprometido hasta el momento.

Análisis de SWPANEL.COM generado por SWPanel

Resumen ejecutivo de seguridad

Los intentos de ataque que se registran en los logs son comunes en internet y no significan necesariamente que el sistema esté comprometido. Sin embargo, las vulnerabilidades reales, aunque no estén actualmente siendo explotadas, son puertas abiertas que pueden ser aprovechadas por atacantes. En este caso, hay dos vulnerabilidades identificadas, ninguna de ellas con un nivel de gravedad extremo, pero que, si se dejan sin abordar, podrían convertirse en puntos de entrada. Además, el sistema tiene algunos errores de código y de SQL que, aunque no son críticos, pueden afectar la estabilidad y la seguridad del sitio. En resumen, aunque la situación no es crítica en este momento, hay aspectos que requieren atención urgente para evitar que el riesgo aumente.

PRIORIDADES

1. **Revisar y parchear las vulnerabilidades identificadas** — URGENTE
   Aunque no están actualmente siendo explotadas, su existencia representa un riesgo potencial que debe abordarse de inmediato.

2. **Revisar y corregir los errores de código y SQL**
   Estos errores pueden afectar la estabilidad del sistema y aumentar la exposición a posibles atacantes.

3. **Analizar las IPs con reputación maliciosa**
   Aunque no se han detectado conexiones activas con servidores de control, es importante comprender el origen de los intentos de ataque y bloquearlas si es necesario.

4. **Revisar la configuración de seguridad del CMS**
   Asegurarse de que WordPress esté correctamente configurado y que se estén siguiendo buenas prácticas de seguridad.

5. **Implementar medidas de monitoreo activo**
   Para detectar y responder rápidamente a cualquier actividad sospechosa en el futuro.

CONTEXTO

Análisis de SWPANEL.COM generado por SWPanel

Resumen ejecutivo de seguridad

Muchos de los intentos de ataque que se registran son parte del ruido habitual en internet y no representan una amenaza directa. Sin embargo, cuando estos intentos se dirigen a vulnerabilidades reales, como las que se han identificado, la situación cambia y se convierte en algo que no se puede ignorar. Afortunadamente, el sistema no muestra señales de que ya esté comprometido, lo cual es un alivio. No obstante, el hecho de que existan vulnerabilidades y errores en el código significa que el sistema no está completamente seguro y que conviene actuar cuanto antes para minimizar el riesgo. Cerrar estas brechas no solo protege el sitio ahora, sino que también reduce la posibilidad de que se conviertan en puntos de entrada en el futuro.

HOJA DE RUTA

1. A corto plazo: Parchear las vulnerabilidades identificadas, corregir los errores de código y SQL, y revisar las IPs con reputación maliciosa. **URGENTE**
2. A medio plazo: Revisar la configuración de seguridad del CMS, implementar medidas de monitoreo activo y realizar una auditoría de seguridad más profunda.
3. A largo plazo: Mantener actualizados todos los componentes del sistema, seguir buenas prácticas de seguridad y realizar revisiones periódicas para garantizar que el sitio siga siendo seguro.

Análisis de SWPANEL.COM generado por SWPanel

02

Resumen del análisis

Errores de código detectados en los logs de Apache/Nginx, su gravedad y los ficheros afectados.

Análisis de SWPANEL.COM generado por SWPanel

Introducción

Esta herramienta analiza automáticamente los logs del servidor web para localizar errores de programación reales que están ocurriendo en producción y proponer su corrección. No es un análisis teórico: trabaja sobre los errores que las visitas están provocando ahora mismo.

Se revisan los logs de las distintas capas del servidor web: los logs proporcionados. Cada petición que falla por un fallo de código deja un rastro en estos logs, con el fichero y la línea exactos donde se produjo.

Qué buscamos: solo errores de programación que se puedan corregir, es decir, los que apuntan a un fichero de código concreto y a una línea. Los accesos normales, los 404 y los problemas de infraestructura (timeouts, upstreams) se descartan automáticamente.

Patrones detectados: errores de PHP (Parse, Fatal, Warning, Notice, Deprecated, Recoverable y excepciones Uncaught) y, en general, cualquier error con una referencia clara a un fichero y una línea (on line N o fichero:N), tanto en Apache como en Nginx.

Cómo trabaja: descarga los logs, los analiza línea a línea, agrupa los errores por fichero afectado y, para cada fichero, el Motor IA de SWPanel, entrenado y especializado en código, propone el diagnóstico de la causa raíz y el fichero ya corregido, listo para revisar y aplicar.

Análisis de SWPANEL.COM generado por SWPanel

Resumen ejecutivo

Síntesis del estado del código según los errores capturados en los logs de Apache/Nginx.

SITUACIÓN

5	5	Tema + plugins
errores únicos	patrones diferentes	componentes afectados

Errores repetidos que afectan a componentes clave del sistema y pueden provocar fallos en la visualización o el funcionamiento de determinadas secciones del sitio.

ERRORES DETECTADOS · POR PRIORIDAD DE CORRECCIÓN

PRIORIDAD

1

Type error tema - template-tags.php

Uncaught TypeError: count(): Argument #1 ($value) must be of type Countable|array, null given

› **Acción:** corregir el tipo de dato pasado a la función; puede afectar la generación de feeds y la indexación del sitio.

PRIORIDAD

2

Memoria agotada plugin - export.php

PHP Fatal error: Allowed memory size of 268435456 bytes exhausted (tried to allocate 20480 bytes)

› **Acción:** revisar y corregir el código afectado para evitar el problema.

PRIORIDAD

3

Acceso a propiedades nulas tema - functions.php

Warning: Attempt to read property "post_title" on null

› **Acción:** verificar y corregir para evitar fallos en la visualización de contenidos.

Análisis de SWPANEL.COM generado por SWPanel

Errores detectados

Lista de errores únicos detectados (las repeticiones se agrupan). Ordenados tal como aparecen en el log.

	Tipo	Fichero	Lín	Mensaje
1	Type error ×37	...theme/inc/template-tags.php	142	Uncaught TypeError: count(): Argument #1 ($value) must be of type Countable|array, null gi
2	Acceso a propiedades nulas ×12	...swpanel-theme/functions.php	88	Warning: Attempt to read property "post_title" on null
3	Clave de array inexistente ×214	.../includes/class-pricing.php	56	Warning: Undefined array key "currency"
4	Deprecated ×1480	.../includes/class-pricing.php	23	Deprecated: Creation of dynamic property SW_Pricing::$plans is deprecated
5	Memoria agotada ×3	...ontact-forms/lib/export.php	301	PHP Fatal error: Allowed memory size of 268435456 bytes exhausted (tried to allocate 20480

Análisis de SWPANEL.COM generado por SWPanel

03

Seguridad y detección de malware

Patrones maliciosos, ofuscación, backdoors y signos de compromiso detectados en el código.

Análisis de SWPANEL.COM generado por SWPanel

Seguridad y detección de malware

Cómo analizamos la seguridad de tu código y cómo interpretar los resultados.

En este capítulo revisamos el código de los ficheros implicados buscando señales de software malicioso: backdoors, webshells, código ofuscado (base64, eval), redirecciones ocultas, spam SEO y otros indicadores de que un fichero ha sido manipulado. El análisis combina dos pasos: un escáner que busca patrones conocidos de malware y una evaluación realizada por el Motor IA de SWPanel, entrenado y especializado en código.

Para cada fichero mostramos los indicadores detectados (con su línea y una descripción) y un veredicto —limpio, sospechoso o comprometido— acompañado de su razonamiento. Las conclusiones se basan en esos indicadores y en el contexto del código, no en suposiciones. Esto te ayuda a saber qué ficheros merecen una revisión prioritaria y por qué, antes de tocar nada.

UNA NOTA IMPORTANTE SOBRE EL MOTOR IA DE SWPANEL

Esta evaluación la genera el Motor IA de SWPanel, nuestro motor inteligente entrenado y especializado en código. Como cualquier motor de este tipo, puede equivocarse: tanto marcar como sospechoso código legítimo como pasar por alto una amenaza real. Tómala como una opinión orientativa, no como un veredicto definitivo. Antes de borrar o modificar cualquier fichero, contrasta sus conclusiones con un profesional o experto en desarrollo web.

Análisis de SWPANEL.COM generado por SWPanel

Seguridad y detección de malware

`/var/www/swpanel.com/datos/web/wp-content/themes/swpanel-theme/inc/template-tags.php`

Veredicto: LIMPIO - sin indicios de compromiso

Motor IA de SWPanel

El archivo ha superado el análisis de seguridad sin detectar código malicioso ni manipulación.

INDICADORES DE LA EVALUACIÓN

No hay eval. base64 ofuscado, webshells ni llamadas a system()/exec().

- webshell
- eval
- base64 ofuscado
- inyecciones
- ejecución remota

El código coincide con la estructura habitual de un tema/plugin de WordPress.

RECOMENDACIÓN

SEGUIMIENTO RECOMENDADO

`inc/template-tags.php`

Aplicar la corrección propuesta y mantener el fichero bajo control de versiones.

Análisis de SWPANEL.COM generado por SWPanel

Seguridad y detección de malware

`/var/www/swpanel.com/datos/web/wp-content/themes/swpanel-theme/functions.php`

Veredicto: LIMPIO - sin indicios de compromiso

Motor IA de SWPanel

El archivo ha superado el análisis de seguridad sin detectar código malicioso ni manipulación.

INDICADORES DE LA EVALUACIÓN

No hay eval. base64 ofuscado, webshells ni llamadas a system()/exec().

- webshell
- eval
- base64 ofuscado
- inyecciones
- ejecución remota

El código coincide con la estructura habitual de un tema/plugin de WordPress.

RECOMENDACIÓN

SEGUIMIENTO RECOMENDADO

`swpanel-theme/functions.php`

Aplicar la corrección propuesta y mantener el fichero bajo control de versiones.

Análisis de SWPANEL.COM generado por SWPanel

Seguridad y detección de malware

`/var/www/swpanel.com/datos/web/wp-content/plugins/sw-pricing-table/includes/class-pricing.ph`

Veredicto: LIMPIO - sin indicios de compromiso

Motor IA de SWPanel

El archivo ha superado el análisis de seguridad sin detectar código malicioso ni manipulación.

INDICADORES DE LA EVALUACIÓN

No hay eval. base64 ofuscado, webshells ni llamadas a system()/exec().

- webshell
- eval
- base64 ofuscado
- inyecciones
- ejecución remota

El código coincide con la estructura habitual de un tema/plugin de WordPress.

RECOMENDACIÓN

SEGUIMIENTO RECOMENDADO

`includes/class-pricing.php`

Aplicar la corrección propuesta y mantener el fichero bajo control de versiones.

Análisis de SWPANEL.COM generado por SWPanel

Seguridad y detección de malware

`/var/www/swpanel.com/datos/web/wp-content/plugins/sw-contact-forms/lib/export.php`

Veredicto: SOSPECHOSO - requiere revisión manual Motor IA de SWPanel

Se han detectado patrones que requieren una revisión manual del archivo.

Indicadores detectados

Severidad	Patrón	Lín	Descripción
ALTO	unserialize($_POST)	118	Deserializa datos enviados por el usuario: puede permitir inyección de objetos PHP.

INDICADORES DE LA EVALUACIÓN

- unserialize() sobre $_POST['filters'] en la línea 118: un atacante podría inyectar objetos PHP.
- No hay indicios de código malicioso: es un fallo de diseño, no una infección.

RECOMENDACIÓN

SEGUIMIENTO RECOMENDADO

`lib/export.php`

Sustituir unserialize() por json_decode() y validar los campos recibidos.

Análisis de SWPANEL.COM generado por SWPanel

04

Correcciones propuestas

Diagnóstico de la causa raíz y código corregido, fichero a fichero, generado por el Motor IA de SWPanel.

Análisis de SWPANEL.COM generado por SWPanel

Fichero 1 de 4

/var/www/swpanel.com/datos/web/wp-content/themes/swpanel-theme/inc/template-tags.php

Lenguaje: php Errores: 1

CORRECCIÓN PROPUESTA

```
Type error (línea 142): Uncaught TypeError: count(): Argument #1 ($value) must be of type
Countable|array, null given
```

DIAGNÓSTICO

En la línea 142 se llama a count() sobre el resultado de get_the_category(). Cuando una entrada no tiene categorías (borradores importados o páginas de producto), la función devuelve null y PHP 8 lanza un TypeError que corta el listado del blog.

CAMBIOS

LÍNEAS 142	Se fuerza un array vacío cuando no hay categorías antes de contarlas.

RIESGO

Bajo: solo cambia el caso sin categorías, que hoy falla.

» Ver el **Código corregido** en la página siguiente.

Análisis de SWPANEL.COM generado por SWPanel

Código corregido

/var/www/swpanel.com/datos/web/wp-content/themes/swpanel-theme/inc/template-tags.php

</> template-tags.php — código actual — corrección propuesta

```
1  1  $cats = get_the_category( $post_id );
-  2+ if ( ! is_array( $cats ) ) {
-  3+     $cats = array();
-  4+ }
2  5  if ( count( $cats ) > 1 ) {
3  6      echo '<span class="cat-list">' . esc_html( $cats[0]->name ) . '</span>';
4  7  }
```

Análisis de SWPANEL.COM generado por SWPanel

Fichero 2 de 4

/var/www/swpanel.com/datos/web/wp-content/themes/swpanel-theme/functions.php

Lenguaje: php Errores: 1

CORRECCIÓN PROPUESTA

```
Acceso a propiedades nulas (línea 88): Warning: Attempt to read property "post_title" on null
```

DIAGNÓSTICO

get_post() devuelve null cuando el ID de la página destacada configurada en el personalizador ya no existe; luego se lee ->post_title sin comprobarlo.

CAMBIOS

LÍNEAS 88	Se comprueba que la entrada exista antes de usar su título.

RIESGO

Bajo.

» Ver el **Código corregido** en la página siguiente.

Análisis de SWPANEL.COM generado por SWPanel

Código corregido

/var/www/swpanel.com/datos/web/wp-content/themes/swpanel-theme/functions.php

</> functions.php — código actual — corrección propuesta

```
1  1  $featured = get_post( get_theme_mod( 'sw_featured_page' ) );
2  -  $title = $featured->post_title;
-  2  $title = $featured instanceof WP_Post ? $featured->post_title : '';
```

Análisis de SWPANEL.COM generado por SWPanel

Fichero 3 de 4

/var/www/swpanel.com/datos/web/wp-content/plugins/sw-pricing-table/includes/class-pricing.php

Lenguaje: php Errores: 2

CORRECCIÓN PROPUESTA

```
Clave de array inexistente (línea 56): Warning: Undefined array key "currency" Deprecated
(línea 23): Deprecated: Creation of dynamic property SW_Pricing::$plans is deprecated
```

DIAGNÓSTICO

La clase SW_Pricing crea la propiedad $plans sin declararla (obsoleto desde PHP 8.2) y lee $opts['currency'] sin valor por defecto cuando el plan no tiene moneda.

CAMBIOS

LÍNEAS 56, 23	Se declara la propiedad y se usa EUR por defecto.

RIESGO

⚠ Nulo: no cambia el comportamiento visible.

» Ver el **Código corregido** en la página siguiente.

Análisis de SWPANEL.COM generado por SWPanel

Código corregido

/var/www/swpanel.com/datos/web/wp-content/plugins/sw-pricing-table/includes/class-pricing.php

</> class-pricing.php — código actual — corrección propuesta

```
 1   1  class SW_Pricing {
 -   2+     public array $plans = array();
 -   3+     public string $currency = 'EUR';
 2   4      public function __construct( $opts ) {
 3   -          $this->plans = $opts['plans'];
 4   -          $this->currency = $opts['currency'];
 -   5+         $this->plans = $opts['plans'] ?? array();
 -   6+         $this->currency = $opts['currency'] ?? 'EUR';
```

Análisis de SWPANEL.COM generado por SWPanel

Fichero 4 de 4

/var/www/swpanel.com/datos/web/wp-content/plugins/sw-contact-forms/lib/export.php

Lenguaje: php Errores: 1

CORRECCIÓN PROPUESTA

```
Memoria agotada (línea 301): PHP Fatal error: Allowed memory size of 268435456 bytes
exhausted (tried to allocate 20480 bytes)
```

DIAGNÓSTICO

La exportación carga todos los envíos del formulario en memoria de una sola vez (unos 61.000) antes de escribir el CSV y supera el límite de 256 MB.

CAMBIOS

LÍNEAS 301	Se lee por lotes de 500 registros y se escribe el CSV a medida.

RIESGO

⚠ Bajo: probar una exportación completa tras aplicarlo.

» Ver el **Código corregido** en la página siguiente.

Análisis de SWPANEL.COM generado por SWPanel

Código corregido

/var/www/swpanel.com/datos/web/wp-content/plugins/sw-contact-forms/lib/export.php

</> export.php — código actual — corrección propuesta

```
- $rows = $wpdb->get_results( "SELECT * FROM {$table}" );
- foreach ( $rows as $r ) {
-     fputcsv( $out, (array) $r );
- }
+ $offset = 0;
+ do {
+     $rows = $wpdb->get_results( $wpdb->prepare( "SELECT * FROM {$table} LIMIT %d, 500"
+     foreach ( $rows as $r ) {
+         fputcsv( $out, (array) $r );
+     }
+     $offset += 500;
+ } while ( count( $rows ) === 500 );
```

Análisis de SWPANEL.COM generado por SWPanel

05

Errores SQL detectados

Sentencias SQL que han fallado según los logs, con la corrección sugerida.

Análisis de SWPANEL.COM generado por SWPanel

Errores SQL detectados

Sentencias SQL que han fallado según los logs, con la corrección sugerida.

• Permisos / conexión BBDD • Falso positivo · log truncado • Corrección propuesta

Error SQL 1 ×642

PERMISOS / CONEXIÓN BBDD

642 apariciones en el log

```
WordPress database error Unknown column 'plan_slug' in 'where clause' for query SELECT * FROM wp_sw_pricing WHERE plan_slug = 'cloud-pro'
```

CONSULTA DETECTADA

```
SELECT * FROM wp_sw_pricing WHERE plan_slug = 'cloud-pro'
```

La columna se renombró a 'slug' en la versión 2.0 del plugin, pero esta consulta sigue usando el nombre antiguo.

CORRECCIÓN PROPUESTA

Conceder permisos de escritura al usuario de BBDD (o revisar la configuración de conexión en wp-config.php).

```
SELECT * FROM wp_sw_pricing WHERE slug = 'cloud-pro'
```

Error SQL 2 ×9

PERMISOS / CONEXIÓN BBDD

9 apariciones en el log

```
WordPress database error Deadlock found when trying to get lock; try restarting transaction for query UPDATE wp_options SET option_value = '...' WHERE option_name = '_transient_sw_rates'
```

CONSULTA DETECTADA

```
UPDATE wp_options SET option_value = '...' WHERE option_name = '_transient_sw_rates'
```

La consulta es correcta: dos procesos de wp-cron actualizan el mismo transient a la vez. Conviene desactivar wp-cron por visita y lanzarlo desde un cron del sistema.

CORRECCIÓN PROPUESTA

Conceder permisos de escritura al usuario de BBDD (o revisar la configuración de conexión en wp-config.php).

Análisis de SWPANEL.COM generado por SWPanel

06

Diagnóstico del tráfico

Explicación en lenguaje sencillo de lo que muestran los logs y acciones recomendadas.

Análisis de SWPANEL.COM generado por SWPanel

Diagnóstico del tráfico

A partir de lo que muestran los logs, aquí tienes el resumen en lenguaje claro y las acciones recomendadas.

Gravedad: ALTA

El sitio está experimentando múltiples intentos de ataque, con acceso a archivos sensibles, inyecciones maliciosas y ataques de fuerza bruta, lo que pone en riesgo su seguridad y estabilidad.

QUÉ ESTÁ PASANDO

Intentos de entrar por fuerza

Alguien prueba contraseñas repetidamente para colarse en el sitio. 418 intentos detectados. Sobre todo desde 203.0.113.77.

Escaneo buscando agujeros

Intentan abrir archivos de configuración sensibles para encontrar puntos débiles. 1312 peticiones.

Intentos de inyección

Peticiones con código malicioso (SQL/XSS) para manipular la web. 23 casos.

Intentos de abrir archivos prohibidos

403

Intentos de acceso a archivos ocultos o sensibles. El servidor los ha bloqueado.

Búsqueda de páginas inexistentes

404

Peticiones a páginas que no existen, a menudo para sondear el sitio. 2870 casos.

Errores internos del servidor

500

El servidor ha tenido problemas para responder, quizá por sobrecarga. 41 errores.

La infraestructura aguanta

Sin timeouts ni errores de conexión entre Nginx y Apache. La infraestructura funciona.

QUÉ HAY QUE HACER

1

Activa la CDN de Cloudflare desde tu SWPanel para filtrar bots, IPs maliciosas y tráfico no deseado antes de que llegue a tu servidor. Esta es la solución más segura y fácil de implementar.

URGENTE

Análisis de SWPANEL.COM generado por SWPanel

Diagnóstico del tráfico

2 **Bloquea manualmente las IPs más agresivas con iptables** si no usas Cloudflare o mientras se activa. Ejemplo para bloquear 203.0.113.45 y 198.51.100.23:

```
iptables -A INPUT -s 203.0.113.45 -j DROP
iptables -A INPUT -s 198.51.100.23 -j DROP
```

3 **Verifica que el Fail2Ban gestionado esté activo** en tu SWPanel para bloquear automáticamente IPs que intenten atacar repetidamente.

4 **Revisa y actualiza la configuración de WordPress** para ocultar archivos sensibles (como .env, .git, wp-config.php.bak) y asegúrate de que el sitio no tenga rutas obsoletas o vulnerables.

5 **Revisa las actualizaciones del CMS y plugins** para asegurarte de que WordPress 6.8.2 esté completamente protegido contra vulnerabilidades conocidas.

Análisis de SWPANEL.COM generado por SWPanel

IP a bloquear

No necesitas tocar nada técnico

Estas son las 5 IP maliciosas que hay que bloquear. La manera más sencilla es hacerlo desde tu SWPanel con un par de clics, sin comandos ni acceso al servidor. Si lo prefieres, más abajo tienes los comandos exactos para tu técnico.

LA FORMA MÁS SENCILLA: ACTIVA LA CDN DE CLOUDFLARE

CDN de Cloudflare — RECOMENDADO

Este servicio no está dentro de un Cloud, así que el FW de Capa 4 no está disponible. Activa la CDN de Cloudflare desde tu SWPanel: hace de proxy y filtra el tráfico malicioso (IP, países y bots) antes de que llegue a tu sitio, sin comandos ni acceso al servidor.

IP A BLOQUEAR

- `203.0.113.77`
- `192.0.2.150`
- `203.0.113.45`
- `198.51.100.23`
- `198.51.100.88`

ALTERNATIVA MANUAL PARA TU TÉCNICO: COMANDOS IPTABLES

```
iptables -A INPUT -s 203.0.113.77 -j DROP
iptables -A INPUT -s 192.0.2.150 -j DROP
iptables -A INPUT -s 203.0.113.45 -j DROP
iptables -A INPUT -s 198.51.100.23 -j DROP
iptables -A INPUT -s 198.51.100.88 -j DROP
```

Cada línea bloquea una IP. Pide a tu técnico que las aplique y las haga permanentes (para que no se pierdan al reiniciar). Y como ya tienes el Fail2Ban Gestionado activo, configúralo en Seguridad > Fail2Ban para que bloquee automáticamente a los futuros atacantes.

Análisis de SWPANEL.COM generado por SWPanel

07

Tráfico y seguridad (logs de acceso)

Hallazgos detectados analizando los logs de acceso del servidor web.

Análisis de SWPANEL.COM generado por SWPanel

Tráfico y seguridad (logs de acceso)

Hallazgos detectados analizando los logs de acceso del servidor web. (186420 peticiones analizadas)

Severidad	Categoría	Nº	Muestra
CRÍTICO	Inyección en la URL	23	
ALTO	Escaneo de ficheros sensibles	1.312	
ALTO	Intentos de acceso / fuerza bruta	418	
ALTO	Errores de servidor (5xx)	41	
MEDIO	Accesos bloqueados (reconocimiento)	356	
MEDIO	Páginas no encontradas (404)	2.870	

Detalle de los accesos detectados

CRÍTICO

Inyección en la URL

23 peticiones

RUTAS PRINCIPALES	ORIGEN (IPS IMPLICADAS)	REPETICIONES
`/?s=%27+union+select+user_login,user_pass`	`198.51.100.23`	17
`/?p=1%3Cscript%3Ealert(1)%3C/script%3E`	`203.0.113.45`	6

ALTO

Escaneo de ficheros sensibles

1.312 peticiones

RUTAS PRINCIPALES	ORIGEN (IPS IMPLICADAS)	REPETICIONES
`/.env`	`203.0.113.45`	610
`/wp-config.php.bak`	`198.51.100.23`	402
`/.git/config`		
`/phpinfo.php`		

Análisis de SWPANEL.COM generado por SWPanel

Tráfico y seguridad (logs de acceso)

Detalle de los accesos detectados (continuación)

ALTO

Intentos de acceso / fuerza bruta

418 peticiones

RUTAS PRINCIPALES	ORIGEN (IPS IMPLICADAS)	REPETICIONES
`POST /wp-login.php`	`203.0.113.77`	296
`POST /xmlrpc.php`	`192.0.2.150`	122

Errores de servidor (5xx) 41

`500 /blog/`
`500 /wp-admin/admin-post.ph`

Páginas no encontradas (404) 2.870

`/precios-antiguos/`
`/wp-content/uploads/2024/03/`

IP principal: 203.0.113.45 (940)

Accesos bloqueados (reconocimiento) 356

`/wp-content/uploads/.htacces`
`/wp-includes/wlwmanifest.xml`

PATRONES DETECTADOS EN LAS MUESTRAS (OWASP CRS)

- Inyección SQL (SQLi): 2
- Ejecución de código (RCE): 8

Recomendaciones prioritarias

CRÍTICO

Inyección en la URL

estos intentos buscan ejecutar SQL o leer ficheros del sistema. Revisa que todas las entradas se validan y se usan consultas parametrizadas, y considera añadir reglas de WAF.

ALTO

Escaneo de ficheros sensibles

bloquea el acceso a rutas como .env, .git, wp-config y phpMyAdmin desde el servidor web o el WAF y comprueba que esos ficheros no son accesibles públicamente.

ALTO

Intentos de acceso / fuerza bruta

limita los intentos de inicio de sesión, activa la autenticación en dos pasos en wp-login y el panel de administración, y bloquea las IPs reincidentes (fail2ban o WAF).

ALTO

Errores de servidor (5xx)

indican fallos del backend o de la aplicación en producción. Revisa los logs de error de las rutas afectadas y corrige la causa para no perder peticiones legítimas.

Análisis de SWPANEL.COM generado por SWPanel

Tráfico y seguridad (logs de acceso)

Recomendaciones prioritarias

MEDIO

Páginas no encontradas (404)

un volumen alto puede indicar enlaces rotos o contenido eliminado. Revisa las URLs más frecuentes y añade redirecciones 301 hacia el destino correcto.

Análisis de SWPANEL.COM generado por SWPanel

08

Errores de JavaScript

Errores reales detectados al cargar tus páginas en un navegador, con el código que falla y su corrección.

Análisis de SWPANEL.COM generado por SWPanel

Errores de JavaScript

Cómo analizamos el JavaScript de tu web y cómo leer los resultados.

Para este análisis cargamos tus páginas en un navegador real (Chromium, sin ventana) y registramos lo que ocurre: errores en la consola, excepciones de JavaScript y recursos que no cargan. Revisamos varias páginas del dominio, tomadas de los registros de acceso (las más visitadas) y del sitemap.xml.

Para cada error mostramos en qué página ocurre, el fichero y la línea, y si es código tuyo (primera parte) o de un servicio externo (terceros). Cuando es código tuyo, mostramos el fragmento que falla y una corrección propuesta. También identificamos las librerías de mercado que usas y cuántos scripts carga cada página, porque un exceso de scripts ralentiza la web.

UNA NOTA IMPORTANTE SOBRE EL MOTOR IA DE SWPANEL

El análisis y las correcciones de este capítulo los genera el Motor IA de SWPanel, entrenado y especializado en código, sobre lo que captura un navegador real. Como cualquier motor de este tipo, puede equivocarse o proponer un cambio que no encaje con tu código. Tómalo como una orientación: antes de aplicar cualquier corrección, pruébala y contrástala con un profesional o experto en desarrollo web.

Análisis de SWPANEL.COM generado por SWPanel

Errores de JavaScript

18 páginas analizadas en un navegador real.

Errores en tu código (primera parte)

TypeError (tu código) ×17

Página: https://swpanel.com/precios/ · https://swpanel.com/wp-content/themes/swpanel-theme/js/pricing-toggle.js

Uncaught TypeError: Cannot read properties of null (reading 'addEventListener')

CÓDIGO CON ERROR

```
document.querySelector('#billing-switch').addEventListener('change', onToggle);
```

CORRECCIÓN PROPUESTA

```
const sw = document.querySelector('#billing-switch');.if (sw) { sw.addEventListener('change', onToggle); }
```

Explicación: El script se carga en todas las páginas, pero el interruptor mensual/anual solo existe en /precios/.

Librerías de JavaScript detectadas

jQuery
3.7.1

Swiper
8.4.7

Carga de scripts por página

Número de scripts que carga cada página. Demasiados scripts —o muy pesados— ralentizan la carga y empeoran la experiencia.

Página	Externos	En línea	Total	Estado
/	24	11	**35**	Demasiados scripts
/precios/	27	13	**40**	Demasiados scripts

Análisis de SWPANEL.COM generado por SWPanel

09

Estado del CMS

Gestor de contenidos detectado, su versión y si está actualizado, desactualizado o sin soporte.

Análisis de SWPANEL.COM generado por SWPanel

Estado del CMS

Detectamos el gestor de contenidos (CMS) de tu web y su versión leyéndolos directamente en el servidor, y los comparamos con la última versión oficial y con la fecha de fin de soporte (EOL). Un CMS sin soporte ya no recibe parches de seguridad y es un riesgo.

Versión del gestor

DÓNDE ESTÁS · INSTALADA

6.8.2

A DÓNDE IR · RECOMENDADA

6.8.3

• Con soporte

Gestor de contenidos: WordPress Fin de soporte (EOL): -

Vulnerabilidades conocidas (CVE)

Se han detectado 1 vulnerabilidades (CVE) públicas que afectan a la versión instalada. CVSS máximo: 5.4 (MEDIUM). Ejemplos: CVE-2026-0000 (5.4). EPSS max: 0%. Muestra reciente de los CVE más nuevos; la cobertura completa requiere el módulo de vulnerabilidades en caché.

Vulnerabilitats conegudes de plugins i temes

1 plugins/temes amb vulnerabilitats conegudes (1 CVE en total). Puntuacio maxima: 6.4 (MEDIUM). Components afectats: contact-form-7 5.9.8 (1 CVE, max 6.4). EPSS max: 0%. Actualitza els plugins i temes a la darrera versio disponible.

Plugins y temas desactualizados

2

• 2 con salto de versión mayor (prioritarios) • 0 con salto menor Total: 2

Componente	Tipo	Instalada	Última	Salto
PRIORITARIOS · SALTO DE VERSIÓN MAYOR				
Contact Form 7	PLUGIN	5.9.8	6.1.1	MAYOR
Yoast SEO	PLUGIN	25.4	26.1	MAYOR

QUÉ SIGNIFICA Y QUÉ HAY QUE HACER

Análisis de SWPANEL.COM generado por SWPanel

Estado del CMS

Su sitio web utiliza el gestor de contenidos WordPress, versión 6.8.2, que actualmente está desactualizado, ya que existe disponible una versión más reciente, la 6.8.3. Actualizar a esta versión recomendada es una buena forma de mantener su sitio seguro y funcional. Un gestor de contenidos desactualizado puede ser comparado con una cerradura que el fabricante ya no mantiene ni mejora: con el tiempo, puede acumular agujeros de seguridad que no se reparan, aumentando el riesgo para su sitio.

En la versión instalada se han identificado 2 vulnerabilidades conocidas, lo que significa que existen fallos de seguridad ya documentados y públicos. Aunque ninguna de estas vulnerabilidades tiene exploit público ni aparece en listas de explotación activa, su gravedad máxima alcanza un nivel 6.4 sobre 10, lo que indica un riesgo moderado. En la práctica, esto podría traducirse en accesos no autorizados a su sitio, robo de información sensible, inyección de contenido no deseado o incluso la caída temporal del sitio, afectando su reputación y la experiencia de sus visitantes.

Lo más recomendable es actualizar el núcleo del gestor de contenidos a la versión 6.8.3, que es la actualización disponible y recomendada. Si bien es prudente probar antes cualquier actualización en un entorno de prueba para evitar sorpresas, mantener el sistema actualizado es una de las medidas más efectivas y económicas para proteger su sitio. Cada actualización resuelve múltiples problemas de seguridad de una sola vez, evitando que los riesgos se acumulen y se conviertan en un problema más grave con el tiempo.

Análisis de SWPANEL.COM generado por SWPanel

Estado del CMS

Hoja de ruta de actualización

Tu situación

Tu versión 6.8.2 se publicó hace un año. La versión actual es la 7.0 (may 2026).

EN POCAS PALABRAS

Actualizar el gestor de contenidos de su sitio web es una inversión en tranquilidad y seguridad. Aunque el tiempo que lleva sin actualizar no sea muy largo, cuanto más se retrase una actualización, más complejo puede volverse el proceso. Si el sistema ha estado sin actualizarse durante varios años, es normal que haya cambios intermedios que no se puedan saltar, y que haya acumulado actualizaciones que ahora hay que aplicar de forma ordenada. Esto no significa que sea un problema grave, sino que hay que abordarlo con paciencia y cuidado. El objetivo es asegurarse de que el sitio siga funcionando bien, con todas sus herramientas y diseños, y que esté protegido contra posibles amenazas.

El camino más seguro para actualizar es hacer una copia de seguridad real, que se pueda restaurar si algo sale mal, y probar la actualización en un entorno de pruebas antes de aplicarla al sitio real. Es importante avanzar paso a paso, sin saltar versiones si el sistema lo recomienda, y comprobar que todo lo que usa en el sitio —como plugins, módulos o diseños— siga funcionando correctamente. Si el salto es grande, puede ser útil contar con ayuda profesional para guiar el proceso. Mantener el gestor actualizado no solo protege el sitio, sino que también evita costos más altos en el futuro. Es una tarea que vale la pena planificar con calma, y que al final resulta mucho más sencilla de lo que parece.

VERSIONES Y FECHAS



Análisis de SWPANEL.COM generado por SWPanel

Estado del CMS

QUÉ NECESITA LA VERSIÓN DESTINO

PHP	Necesitas PHP 8.3 o superior (el mínimo absoluto es 7.4, pero ya está sin soporte). Lo ideal es 8.4.
Base de datos	MySQL 8.0 o superior, o bien MariaDB 10.6 o superior (recomendado).
Memoria / RAM	El fabricante no publica un mínimo de RAM oficial.
Otros requisitos	HTTPS obligatorio. Servidor Apache 2.4 o Nginx 1.26 o superior.

Requisitos según la documentación oficial del fabricante: https://wordpress.org/about/requirements/

PASOS RECOMENDADOS

1

Haz una copia de seguridad completa y comprueba que se puede restaurar

Antes de tocar nada, guarda una copia de todo el sitio: los archivos (tema, plugins y la carpeta de subidas) y también la base de datos, que es donde están los textos y la configuración. Puedes hacerlo desde el panel de tu alojamiento (a menudo hay un botón Copia de seguridad) o pidiéndolo al soporte del proveedor; si tienes un plugin de copias, lanza una copia completa y descárgala en tu ordenador. Lo más importante es comprobar que la copia se puede restaurar de verdad: si puedes, recupérala en una copia de pruebas antes de continuar.

Guía oficial de copias de seguridad
https://developer.wordpress.org/advanced-administration/security/backup/

2

Pon al día el servidor: PHP 8.3 o superior y la base de datos recomendada

WordPress 7.0 requiere un servidor moderno: PHP 8.3 o superior y la base de datos en MariaDB 10.6 o superior, o bien MySQL 8.0 o superior. No tienes que tocar código: estos cambios se hacen desde el panel de tu alojamiento, en una sección como Versión de PHP, o pidiéndolo al soporte del proveedor. Comprueba qué versión tienes ahora y, si va atrasada, pide que la suban a la recomendada. Evita quedarte en versiones antiguas de PHP marcadas como fuera de servicio, porque son un riesgo de seguridad.

Requisitos oficiales de WordPress
https://wordpress.org/about/requirements/

Análisis de SWPANEL.COM generado por SWPanel

Estado del CMS

3

Prueba primero en un entorno de pruebas y revisa tema y plugins

No hagas la actualización directamente sobre el sitio real: haz una copia de pruebas (muchos alojamientos tienen un botón Staging) y actualiza allí primero. En esta copia, desactiva temporalmente los plugins y comprueba si el tema y cada plugin son compatibles con la nueva versión: en Plugins, dentro del administrador, verás avisos de tipo Compatible o No probado con tu versión. Revisa especialmente los plugins antiguos o que ya no reciben actualizaciones, que son los que suelen dar problemas.

Probar WordPress en pruebas
https://developer.wordpress.org/advanced-administration/debug/test-driving/

4

Actualiza el núcleo de WordPress, mejor por etapas si vas muy atrasado

Una vez hecho el paso de pruebas, actualiza el núcleo entrando en el administrador y yendo a Escritorio -> Actualizaciones, donde encontrarás el botón Actualizar ahora. Como ya tienes copia de seguridad puedes dar el salto, pero si tu versión actual es muy antigua es más seguro subir por etapas (de versión importante en versión importante) en lugar de hacer un solo salto grande. Comprueba después que la página principal y el administrador cargan bien. Evita cerrar el navegador mientras se está actualizando.

Guía oficial de actualización
https://developer.wordpress.org/advanced-administration/upgrade/upgrading/

5

Cierra: actualiza la base de datos, reactiva los plugins y vacía la memoria caché

Después de actualizar, si WordPress muestra una pantalla que dice que hay que actualizar la base de datos, haz clic en el botón que te indica para completarla. A continuación vuelve a Plugins y reactiva uno a uno los plugins que habías desactivado, comprobando que el sitio sigue funcionando en cada paso. Finalmente, vacía la memoria caché (en tu plugin de caché o en el panel del alojamiento) para que los visitantes vean la versión nueva. Si algo falla, recuerda que tienes la copia de seguridad para volver atrás.

Gestionar y reactivar plugins
https://wordpress.org/documentation/article/manage-plugins/

Cuenta

A diferencia del resto, WordPress permite actualizar directamente a la última versión si tienes copia de seguridad; aun así, si vas muy atrasado es más seguro hacerlo por etapas.

Fuente: https://wordpress.org/documentation/article/updating-wordpress/

Análisis de SWPANEL.COM generado por SWPanel

Estado del CMS

Componentes no verificables (no están en el repositorio oficial)

3 componentes

No están en el repositorio oficial

No se puede comparar su versión con ninguna fuente oficial. Pueden ser de pago o del propio tema (normal), o bien código añadido sospechoso. Revisa en el capítulo Seguridad los que aparezcan marcados como maliciosos.

Componente	Tipo	Versión instalada
PLUGINS 2		
`sw-pricing-table`	PLUGIN	2.0.3
`sw-contact-forms`	PLUGIN	1.4.0
TEMAS 1		
`swpanel-theme`	THEME	3.2.0

Recomendación

mantén el CMS, los plugins y los temas siempre actualizados y elimina los que no uses. Es la forma más eficaz y económica de proteger tu web.

Análisis de SWPANEL.COM generado por SWPanel

10

Versión y soporte de PHP

La versión de PHP con la que funciona tu sitio y si todavía recibe actualizaciones de seguridad.

Análisis de SWPANEL.COM generado por SWPanel

Versión y soporte de PHP

La versión de PHP con la que funciona tu sitio y si todavía recibe actualizaciones de seguridad.

PHP 8.1.31 fuera de soporte
Esta versión de PHP ya no recibe actualizaciones de seguridad (fin de soporte 31/12/2025). Actualiza a una versión mantenida desde tu SWPanel para recibir parches de seguridad.

display_errors = On
Los errores PHP se muestran al visitante y pueden revelar rutas internas. Desactívalo en producción.

expose_php = On
La cabecera X-Powered-By anuncia la versión exacta de PHP.

Análisis de SWPANEL.COM generado por SWPanel

11

Integridad del núcleo de WordPress

Comparamos los ficheros principales del núcleo de WordPress con los oficiales de wordpress.org (por suma de verificación md5).

Análisis de SWPANEL.COM generado por SWPanel

Integridad del núcleo de WordPress

Comparamos los ficheros principales del núcleo de WordPress con los oficiales de wordpress.org (por suma de verificación md5).

El núcleo coincide con el oficial

Se han verificado 1284 ficheros clave del núcleo; 0 difieren del oficial. No se ha detectado ninguna alteración en los ficheros verificados.

Análisis de SWPANEL.COM generado por SWPanel

12

Exposición y superficie de ataque

Comprobaciones activas del dominio desde el exterior: TLS, cabeceras de seguridad, archivos expuestos y autenticación de correo.

Análisis de SWPANEL.COM generado por SWPanel

Exposición y superficie de ataque

Comprobaciones activas del dominio desde el exterior: TLS, cabeceras de seguridad, archivos expuestos y autenticación de correo.

Resumen del sondeo

TLS: TLS 1.3. Cabeceras de seguridad: 70/100. Subdominios públicos (crt.sh): 3.

Falta Content-Security-Policy

Sin CSP, un script inyectado se ejecutaría sin restricciones.

staging.swpanel.com accesible sin contraseña

El entorno de pruebas es público e indexable; protégelo con contraseña o restricción por IP.

SPF / DKIM / DMARC

SPF y DKIM correctos; DMARC en modo p=none (solo informa).

Análisis de SWPANEL.COM generado por SWPanel

13

Directivas maliciosas de configuración

Análisis del fichero .htaccess en la raíz del sitio: directivas que ocultan código, ejecutan PHP donde no debe o exponen carpetas.

Análisis de SWPANEL.COM generado por SWPanel

Directivas maliciosas de configuración

Análisis del fichero .htaccess en la raíz del sitio: directivas que ocultan código, ejecutan PHP donde no debe o exponen carpetas.

Listado de directorios activado

Options +Indexes expone el contenido de las carpetas sin índice. Desactívalo para no revelar ficheros internos. [Options +Indexes +FollowSymLinks]

Análisis de SWPANEL.COM generado por SWPanel

14

Ataques detectados en los registros

Peticiones en los registros de acceso que coinciden con vectores de ataque conocidos.

Análisis de SWPANEL.COM generado por SWPanel

Ataques detectados en los registros

Peticiones en los registros de acceso que coinciden con vectores de ataque conocidos.

Intentos de explotación detectados

Se han detectado 386 intentos de explotación de vulnerabilidades conocidas; 9 de ellos dirigidos contra vulnerabilidades que afectan a esta web.

Los registros de acceso del sitio web muestran que ha recibido 386 intentos de ataque automatizados en un periodo de tiempo no especificado. La mayoría de estos intentos son ataques genéricos que buscan vulnerabilidades comunes en plataformas como WordPress, y no necesariamente están dirigidos a esta web en particular. Es común que las webs reciban este tipo de tráfico malicioso, ya que los atacantes utilizan herramientas automatizadas para probar miles de objetivos al mismo tiempo. La diferencia clave entre un intento fallido y un ataque real contra esta web radica en si el sistema es vulnerable a la técnica utilizada. En este caso, 9 de los intentos sí afectan a una vulnerabilidad real del sitio, por lo que requieren atención inmediata. Aunque la situación no indica que el sitio ya haya sido comprometido, es fundamental actuar con rapidez para evitar consecuencias graves.

ATAQUES DETECTADOS

CRÍTICO

9 intentos

Contact Form 7 - subida de fichero sin validar (CVE-2026-0000)

El atacante intentó subir archivos no validados a través del plugin Contact Form 7, desde la IP 198.51.100.23, 9 veces. Esta web es vulnerable a este ataque.

ALTO

296 intentos

Fuerza bruta contra wp-login.php

El atacante intentó adivinar credenciales de acceso al panel de WordPress, desde la IP 203.0.113.77, 296 veces. Esta web no es vulnerable a este ataque.

ALTO

17 intentos

Inyección SQL genérica (union select)

El atacante intentó ejecutar comandos SQL maliciosos para extraer información de la base de datos, desde la IP 198.51.100.23, 17 veces. Esta web no es vulnerable a este ataque.

MEDIO

64 intentos

Lectura de ficheros sensibles (.env / wp-config)

El atacante intentó acceder a archivos de configuración que podrían contener claves secretas, desde la IP 203.0.113.45, 64 veces. Esta web no es vulnerable a este ataque.

Análisis de SWPANEL.COM generado por SWPanel

Ataques detectados en los registros

IMPLICACIONES

De los intentos detectados, el más preocupante es el relacionado con la vulnerabilidad en el plugin Contact Form 7. Si este ataque tuviera éxito, el atacante podría subir archivos maliciosos, como scripts de acceso remoto (webshell), que le permitirían controlar el servidor web, ejecutar comandos, robar datos sensibles o incluso usar el sitio como punto de salida para atacar otras redes. Esto podría llevar a una completa toma de control del sitio, con consecuencias como la pérdida de datos, daño a la reputación del cliente o incluso el uso del sitio para actividades ilegales. Aunque los otros intentos no afectan directamente a esta web, no deben ignorarse, ya que podrían ser el preludio de ataques más sofisticados en el futuro.

QUÉ HACER

1. **Parchear el plugin Contact Form 7** — URGENTE

   Aplicar el parche para el CVE-2026-0000 lo antes posible, ya que el sitio es vulnerable a este ataque.

2. **Bloquear las IPs 198.51.100.23 y 203.0.113.77**

   Configurar reglas en el WAF o en Fail2Ban para evitar que estas direcciones accedan al sitio.

   ```
   fail2ban-client set wordpress-attack addip 198.51.100.23
   fail2ban-client set wordpress-attack addip 203.0.113.77
   ```

3. **Revisar si ya hubo compromiso**

   Analizar los logs de sistema, base de datos y archivos del servidor para detectar signos de intrusión, como archivos inusuales o cambios en permisos.

4. **Activar el WAF Adaptativo**

   Asegurarse de que el módulo "Seguridad 360 > WAF Adaptativo" esté activado en el panel de administración.

5. **Monitorizar el tráfico entrante**

   Configurar alertas para detectar patrones similares en el futuro y revisar los logs regularmente.

Análisis de SWPANEL.COM generado por SWPanel

Ataques detectados en los registros

CONTRAMEDIDAS

Contact Form 7 - subida de fichero sin validar (CVE-2026-0000):

- **Inmediata:** Aplicar el parche del CVE-2026-0000 y bloquear la IP 198.51.100.23.

- **Técnica:** Validar todas las entradas de usuario y restringir las extensiones de archivo permitidas.

- **SWPanel:** Activar el WAF Adaptativo en "Seguridad 360" y, si es necesario, añadir la IP a "IPs bloqueadas" en "FireWall de Capa 4".

- **Endurecimiento:** Mantener actualizados todos los plugins y temas, y hacer copias de seguridad periódicas.

Fuerza bruta contra wp-login.php:

- **Inmediata:** Bloquear la IP 203.0.113.77 con WAF o Fail2Ban.

- **Técnica:** No aplica, ya que el sitio no es vulnerable.

- **SWPanel:** Activar el WAF Adaptativo en "Seguridad 360".

- **Endurecimiento:** No aplica.

Inyección SQL genérica (union select):

- **Inmediata:** Bloquear la IP 198.51.100.23 con WAF o Fail2Ban.

- **Técnica:** No aplica, ya que el sitio no es vulnerable.

- **SWPanel:** Activar el WAF Adaptativo en "Seguridad 360".

- **Endurecimiento:** No aplica.

Lectura de ficheros sensibles (.env / wp-config):

- **Inmediata:** Bloquear la IP 203.0.113.45 con WAF o Fail2Ban.

- **Técnica:** No aplica, ya que el sitio no es vulnerable.

- **SWPanel:** Activar el WAF Adaptativo en "Seguridad 360".

Análisis de SWPANEL.COM generado por SWPanel

Ataques detectados en los registros

- **Endurecimiento:** No aplica.

Análisis de SWPANEL.COM generado por SWPanel

15

Tráfico e indicadores de red maliciosos

IPs que han accedido a la web y figuran en listas de infraestructura maliciosa conocida.

Análisis de SWPANEL.COM generado por SWPanel

Tráfico e indicadores de red maliciosos

IPs que han accedido a la web y figuran en listas de infraestructura maliciosa conocida.

IPs maliciosas han accedido a la web

3 IP que figuran en listas de reputación maliciosa (botnets, atacantes, salidas Tor) han hecho peticiones a la web.

3	3
IPs maliciosas que han accedido	con reputación negativa

IP	PAÍS / ASN	CATEGORÍA	FUENTE	PETICIONES
203.0.113.77		Atacante	blocklist_de	296
198.51.100.23		Atacante	abuseipdb	419
192.0.2.150		Salida Tor	tor	122

Se han identificado tres IPs con reputación maliciosa que han accedido al sitio web del cliente. Dos de ellas pertenecen a atacantes conocidos, y una es una salida de la red Tor. En total, estas IPs han realizado 837 peticiones al sitio. Este tipo de tráfico es común en cualquier web y no implica necesariamente que el sitio esté comprometido, pero sí indica que ha sido un objetivo de escaneo o ataque automatizado. Aunque aisladamente esta sección es menos alarmante, el nivel global del sitio sigue siendo ALTO, por lo que se debe actuar con prudencia y priorizar las medidas de mitigación.

NIVEL DE RIESGO

El tráfico hostil entrante, como el proveniente de IPs con reputación de atacantes o salidas Tor, es una señal de que el sitio ha sido escaneado o atacado. Sin embargo, no implica necesariamente un compromiso activo del servidor. Lo más grave sería la comunicación con un C2 de malware, pero en este caso no se han encontrado indicadores de este tipo. A pesar de que esta sección específica no muestra actividad de compromiso, el nivel global del sitio sigue siendo ALTO, por lo que se deben tomar medidas inmediatas para mitigar el riesgo y prevenir posibles intrusiones futuras.

CÓMO MITIGARLO

Análisis de SWPANEL.COM generado por SWPanel

Tráfico e indicadores de red maliciosos

1

1. Activar la CDN de Cloudflare

URGENTE

La CDN de Cloudflare actúa como proxy y filtra IPs maliciosas, bots y tráfico no deseado antes de que llegue al servidor. Es la solución más efectiva y fácil de implementar para este tipo de hosting.

```
Acción: Activar Cloudflare desde el SWPanel del cliente (Configuración > CDN > Activar Cloudflare).
```

2

2. Bloquear IPs con reputación de atacante

Se recomienda bloquear manualmente las IPs con reputación de alto riesgo para evitar futuras conexiones.

```
iptables -A INPUT -s 203.0.113.77 -j DROP
iptables -A INPUT -s 198.51.100.23 -j DROP
```

3

3. Configurar reglas de Fail2Ban gestionado

Aprovechar que Fail2Ban gestionado está activo para configurar reglas personalizadas que bloqueen automáticamente IPs con comportamiento sospechoso.

```
Acción: Configurar reglas personalizadas en Fail2Ban gestionado para IPs con múltiples intentos de acceso.
```

4

4. Monitorizar el tráfico entrante

Es fundamental mantener un registro de las conexiones y revisar periódicamente los logs para detectar patrones inusuales.

```
tcpdump -i eth0 -w /var/log/web_traffic.pcap
```

5

5. Revisar el estado general del sitio

Dado que el nivel global de riesgo es ALTO, se recomienda una auditoría completa del servidor para descartar cualquier posible compromiso.

```
Acción: Revisar logs de acceso, buscar archivos sospechosos y escanear con herramientas de detección de malw
```

Análisis de SWPANEL.COM generado por SWPanel

16

Matriz de Impacto en Negocio

Traducimos cada incidencia técnica detectada a su consecuencia real para tu negocio.

Análisis de SWPANEL.COM generado por SWPanel

Matriz de Impacto en Negocio

Traducimos cada incidencia técnica detectada a su consecuencia real para tu negocio.

INCIDENCIA	IMPACTO TÉCNICO	IMPACTO EN EL NEGOCIO
Bucle de errores PHP Detectado en este sitio	Escritura masiva en el registro de errores y consumo continuo de procesos PHP de tu suscripción.	**Pérdida de clientes:** la web responde lenta o muestra pantallas en blanco intermitentes.
Inyección de código o malware Detectado en este sitio	Funciones no autorizadas ejecutando comandos e hilos en segundo plano.	**Daño de reputación:** Google puede penalizar o desindexar la web, o los antivirus bloquear el acceso a tus visitas.
Consultas SQL fallidas Detectado en este sitio	Incapacidad de leer o escribir registros en el motor de base de datos.	**Pérdida de ventas:** formularios que no se envían y carritos que fallan en el pago.

Análisis de SWPANEL.COM generado por SWPanel

17

Conclusiones

Qué significa todo esto para ti, explicado de forma sencilla.

Análisis de SWPANEL.COM generado por SWPanel

Conclusiones

Qué significa todo esto para ti, explicado de forma sencilla.

Imagínate que tu sitio web es como una casa: tiene puertas, ventanas, un sistema de alarma y una cerradura. Lo que acabamos de ver es que, aunque la casa no está completamente abierta, hay algunas grietas por las que ya están metiendo la nariz personas que no deberían estar ahí. En total, tu web está en un estado de **riesgo ALTO**, lo que significa que no solo hay señales de intentos de ataque, sino también de vulnerabilidades que pueden ser aprovechadas. No es un problema que se pueda ignorar, pero sí uno que se puede solucionar con pasos claros y rápidos.

Lo que está pasando es que tu sitio está siendo atacado de varias formas: bots están intentando adivinar contraseñas, están buscando archivos sensibles como .env o wp-config.php.bak, y están probando si hay agujeros en el código para inyectar comandos maliciosos. Además, hay errores en el código del sitio que pueden hacer que el servidor se bloquee o que se ralentice, y un plugin o tema está usando una versión antigua con una vulnerabilidad conocida. Todo esto juntos crea un entorno donde es más fácil que algo malo ocurra.

Aunque no hay evidencia de que el sitio ya esté completamente comprometido (como un robo de datos o un redireccionamiento malicioso), sí hay señales de que alguien ya está intentando entrar. Por ejemplo, se han detectado más de 1.300 intentos de rastreo agresivo, 418 intentos de fuerza bruta para adivinar contraseñas, y 23 intentos de inyección SQL o XSS. Eso es como si alguien estuviera probando todas las cerraduras de tu casa con ganzúas diferentes, una tras otra.

Lo más urgente es actuar sobre los errores de seguridad y los plugins desactualizados, ya que son puertas que pueden estar abiertas. También es importante reforzar el acceso al sitio para evitar que los bots sigan intentando entrar. Afortunadamente, hay herramientas ya activas, como el sistema de bloqueo automático de atacantes repetidos, que ya están ayudando. Con un plan claro, todo esto se puede resolver.

QUÉ HEMOS ENCONTRADO · POR GRAVEDAD

MEDIO

Errores críticos en el código del sitio

Se han encontrado 5 errores en 4 archivos que pueden causar que el sitio deje de funcionar o que se ralentice. Por ejemplo, uno de ellos hace que el servidor se quede sin memoria al intentar exportar datos, lo que puede afectar a la experiencia del usuario.

CRÍTICO

23 intentos

Intentos de inyección SQL y XSS

Se han detectado 23 intentos de inyección de código malicioso, como intentos de robar contraseñas o inyectar scripts en la web. Esto indica que alguien está intentando aprovechar posibles agujeros en el sistema.

Análisis de SWPANEL.COM generado por SWPanel

Conclusiones

MEDIO

1.312 peticiones

Rastreo agresivo y escaneo de archivos

Más de 1.300 intentos de acceso a archivos sensibles como .env o wp-config.php.bak han sido registrados. Esto sugiere que bots están buscando información sensible que podría comprometer la seguridad del sitio.

ALTO

2 por actualizar

Plugins o temas desactualizados

Dos plugins o temas no están actualizados, y uno de ellos tiene una vulnerabilidad conocida con puntuación de riesgo 5.4. Esto significa que podría ser explotado por atacantes si no se actualiza.

MEDIO

2 errores BD

Errores en la base de datos

Se han encontrado 2 errores relacionados con consultas SQL, lo que puede indicar que el sitio no está usando correctamente la base de datos, lo que puede afectar su rendimiento o seguridad.

PLAN DE ACCIÓN · PASOS A SEGUIR

1

Actualizar plugins o temas desactualizados

URGENTE

Es fundamental actualizar los plugins o temas que no están actualizados, especialmente aquellos con vulnerabilidades conocidas. Esto cierra puertas potenciales de entrada para atacantes.

2

Revisar y corregir errores críticos en el código

Trabajar con un desarrollador para corregir los errores en los archivos template-tags.php, functions.php, class-pricing.php y export.php para evitar que el sitio se bloquee o se ralentice.

Análisis de SWPANEL.COM generado por SWPanel

Conclusiones

3

Configurar reglas de bloqueo en Apache/Nginx

Añadir reglas para bloquear IPs que hayan realizado múltiples intentos de ataque. Por ejemplo, las IPs 203.0.113.45 y 198.51.100.23 han sido especialmente activas.

```
# Ejemplo de bloqueo en Apache (en .htaccess)
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteCond %{REMOTE_ADDR} ^203\.0\.113\.45$
RewriteRule ^ - [F]
</IfModule>
```

4

Activar la CDN de Cloudflare

Usar la CDN de Cloudflare a través de SWPanel para filtrar tráfico malicioso antes de que llegue al servidor. Esto actúa como una capa adicional de seguridad sin necesidad de cambiar configuraciones complicadas.

5

Revisar permisos de archivos y directorios

Asegurarse de que archivos sensibles como .env o wp-config.php.bak no estén accesibles públicamente y que los permisos de los directorios sean estrictos.

Entiendo que esto puede parecer abrumador, pero no estás solo. La situación es grave, pero manejable. Lo más importante es actuar con prioridad en los puntos que ya te he señalado, especialmente en los plugins desactualizados y en los errores críticos del código. Cada paso que des ahora ayuda a cerrar una puerta que un atacante podría usar.

Si necesitas apoyo en cualquiera de estos pasos, ya sea para corregir el código, bloquear IPs o actualizar plugins, estaré encantado de acompañarte en cada uno. Solo tienes que decirme por dónde quieres empezar. El primer paso es clave: actualiza los plugins o temas desactualizados. Eso ya te dará una capa de protección inmediata. Juntos podemos dejar tu sitio seguro y fuerte.

Análisis de SWPANEL.COM generado por SWPanel

Glosario de términos

Breve explicación de los términos técnicos utilizados en este análisis.

Backdoor (puerta trasera)
código oculto que permite a un atacante acceder y controlar el sitio web de forma remota.

Cloaking
mostrar a los buscadores un contenido distinto del que ven los visitantes; típico del spam SEO.

Cuantización
compresión del modelo del Motor IA de SWPanel para que ocupe menos memoria manteniendo casi la misma precisión.

Códigos de estado HTTP (404, 5xx)
404 = página no encontrada; 5xx = error del servidor al procesar la petición.

Fuerza bruta
intentos masivos de adivinar una contraseña probando muchas combinaciones.

Inyección (SQL / URL)
introducir código o comandos a través de un campo o una URL para ejecutar acciones no previstas.

Ofuscación
técnica para ocultar lo que realmente hace el código (por ejemplo con base64_decode) y evitar su detección.

Permisos de BD (GRANT)
privilegios que determinan qué puede hacer un usuario en la base de datos (INSERT, UPDATE...).

Spam SEO
páginas o enlaces inyectados (apuestas, farmacia...) para posicionar contenido fraudulento en tu dominio.

Timeout
la petición tarda demasiado y se interrumpe antes de completarse.

Token
unidad mínima de texto (palabra o fragmento) que procesa el Motor IA de SWPanel; mide el volumen de cálculo.

Transient (WordPress)
dato temporal que WordPress guarda en caché en la base de datos.

Veredicto (Limpio / Sospechoso / Comprometido)
clasificación de seguridad que el análisis asigna a cada fichero.

Análisis de SWPANEL.COM generado por SWPanel

Glosario de términos

Webshell
script malicioso que da al atacante una consola para ejecutar comandos en el servidor.

Análisis de SWPANEL.COM generado por SWPanel

Estadísticas técnicas

Recursos y cómputo invertidos en generar este análisis: descarga y análisis de logs e inferencia del Motor IA de SWPanel.

Tiempo de ejecución

9m 26s	6m 28s	2m 58s
TIEMPO TOTAL	TIEMPO DE ANÁLISIS	CONFECCIÓN DEL PDF

Logs analizados

14	186.420	39,93 MB
LOGS DESCARGADOS	LÍNEAS ANALIZADAS	DATOS PROCESADOS

los logs proporcionados
ORÍAS REVISADAS

Errores y correcciones

5	4	4
ERRORES ÚNICOS	FICHEROS AFECTADOS	CORRECCIONES

2
ERRORES CRÍTICOS

Cómputo del Motor IA de SWPanel

7	11.589	6.054
LLAMADAS AL MODELO	TOKENS DE ENTRADA	TOKENS GENERADOS

17.643	~45 tok/s
TOKENS PROCESADOS	VELOCIDAD DE GENERACIÓN

Análisis de SWPANEL.COM generado por SWPanel

Estadísticas técnicas

Motor IA de SWPanel (análisis y redacción)

qwen3-coder	qwen3moe	30.5B
MOTOR IA DE SWPANEL	FAMILIA	PARÁMETROS

Q8_0
CUANTIZACIÓN

Infraestructura de cómputo

NVIDIA A100	6.912	432
GPU	NÚCLEOS GPU (CUDA)	TENSOR CORES

80 GB HBM2e	2 TB/s	19,5 TFLOPS
VRAM	ANCHO DE BANDA	FP32

312 TFLOPS	221.184	80
FP16/BF16	HILOS CUDA	HILOS DE CPU

Energía consumida y su coste

0,062 kWh	0,093 kWh	0,155 kWh
CONSUMO IT (SERVIDOR + GPU)	REFRIGERACIÓN (X1,5)	ENERGÍA TOTAL

0,19 €
COSTE DE CÓMPUTO

Coste de infraestructura (amortización)

0,61 €	0,155 kWh	38 g
AMORTIZACIÓN HW Y RED	ENERGÍA DE INFRAESTRUCTURA	CO2 DE INFRAESTRUCTURA

Análisis de SWPANEL.COM generado por SWPanel

Estadísticas técnicas

0,83 €
COSTE TOTAL ESTIMADO

77 g
CO2 ESTIMADO

CÓMO SE HAN CALCULADO ESTAS CIFRAS

Métricas estimadas sobre infraestructura NVIDIA NVIDIA A100 con el modelo qwen3-coder:30b-a3b-q8_0. El consumo medio del servidor con la GPU es de unos 575 W. La refrigeración añade 1,5 kW por cada kW de cómputo, así que el consumo total es ~1,5 veces el de cómputo (PUE 1,5). La energía se calcula sobre el tiempo real de análisis a 0,185 EUR/kWh, el coste de cómputo a tarifa cloud de referencia (~1,8 EUR/h) y el CO2 a 250 g/kWh. Valores aproximados para dimensionar el esfuerzo de este análisis.

TECNOLOGÍA EFICIENTE

Este análisis se ejecuta en infraestructura propia con el Motor IA de SWPanel (modelos locales), sin enviar tu código a terceros. Detectar y corregir los errores pronto evita reprocesos, páginas caídas y consumo innecesario de recursos del servidor.

UN GESTO DE AMOR POR EL PLANETA

Crear este informe ha dejado una huella de unos 77 g de CO2. Detrás de cada análisis hay energía, agua y recursos de la única casa que todos compartimos. Te pedimos un pequeño acto de amor: pide solo los informes que de verdad necesites y evita imprimirlos, para cuidar los bosques, el aire y la vida de quienes vendrán después. Cuidar la Tierra es cuidarnos los unos a los otros. Gracias, de corazón, por dejar una huella más ligera y un mañana más verde.

Análisis de SWPANEL.COM generado por SWPanel

swpanel

https://www.swpanel.com

Documento: SW-COD-EJEMPLO-2026

Fecha: 16/10/2026