swpanel

ANÁLISIS DE CÓDIGO Y CORRECCIÓN AUTOMÁTICA · STANDARD

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 del análisis **2**

Introducción 3
Resumen ejecutivo 4
Errores detectados 5

02 Seguridad y detección de malware **6**

Cómo funciona este análisis 7
template-tags.php 8
functions.php 9
class-pricing.php 10
export.php 11

03 Correcciones propuestas **12**

template-tags.php 13
functions.php 15
class-pricing.php 17
export.php 19

04 Errores SQL detectados **21**

05 Diagnóstico del tráfico **23**

06 Tráfico y seguridad (logs de acceso) **27**

07 Errores de JavaScript **31**

Cómo funciona este análisis 32

08 Estado del CMS **34**

09 Exposición y superficie de ataque **40**

10 Conclusiones **42**

Glosario de términos **46**

Estadísticas técnicas **48**

Análisis de SWPANEL.COM generado por SWPanel

01

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

02

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

03

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

04

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

05

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, incluyendo escaneos agresivos, inyección de código malicioso 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 el SWPanel** para filtrar tráfico malicioso, bloquear bots y mejorar la seguridad del sitio. Esta es la solución más efectiva y fácil de implementar. URGENTE

2. **Revisa y reforzaza las contraseñas de administrador en WordPress**, especialmente si usas el mismo nombre de usuario que antes.

Análisis de SWPANEL.COM generado por SWPanel

Diagnóstico del tráfico

3 **Bloquea las IPs más activas en ataques** usando Fail2Ban gestionado (ya activo), que puede bloquear automáticamente IPs que intenten fuerza bruta repetidamente. Si no se bloquean automáticamente, puedes añadirlas manualmente con esta regla

```
iptables -A INPUT -s 203.0.113.77 -j DROP
iptables -A INPUT -s 192.0.2.150 -j DROP
```

4 **Bloquea manualmente las IPs que realizan escaneos agresivos** si no se filtran con Cloudflare. Puedes usar esta regla iptables:

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

5 **Revisa la configuración de WordPress** para deshabilitar el acceso a archivos sensibles como .env, wp-config.php.bak o .git/config. Puedes usar .htaccess para prohibir el acceso a estos archivos si no son necesarios.

6 **Monitorea los logs regularmente** para detectar nuevos patrones de ataque y ajustar las medidas de seguridad.

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

06

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`

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

07

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

08

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

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).

VERSIONES Y FECHAS

- **6.8.2** abr 2025 — PHP 7.2+ · MySQL 5.7+ / MariaDB 10.4+ — TU VERSIÓN
- **6.9** dic 2025 — PHP 7.2+ · MySQL 5.7+ / MariaDB 10.4+ — PASO INTERMEDIO
- **7.0** may 2026 — PHP 7.4+ · MySQL 8.0+ / MariaDB 10.6+ — VERSIÓN ACTUAL

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/

Análisis de SWPANEL.COM generado por SWPanel

Estado del CMS

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/

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/

Análisis de SWPANEL.COM generado por SWPanel

Estado del CMS

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/

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

Análisis de SWPANEL.COM generado por SWPanel

Estado del CMS

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

09

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

10

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. En este momento, hay señales claras de que alguien ha estado husmeando por las ventanas, intentando entrar, y en algunos casos, ya ha dejado rastros de su presencia. Aunque no hay evidencia de que el atacante esté ahora mismo dentro, sí hay indicios de que podría volver si no tomamos medidas. Lo que hemos encontrado en el análisis es grave, pero no imposible de solucionar. Tu web no está completamente comprometida, pero sí está en un estado de riesgo alto, y eso significa que debes actuar con urgencia.

Lo primero que debes saber es que tu sitio está siendo atacado de varias formas: bots están intentando adivinar contraseñas, otros están buscando agujeros en el código para inyectar contenido malicioso, y hay intentos de acceder a archivos sensibles que podrían revelar información importante. Además, tu sitio tiene errores en el código que no solo afectan el funcionamiento, sino que también pueden facilitar que los atacantes exploren más fácilmente. Por ejemplo, hay un error de memoria agotada que podría ser aprovechado para causar caídas o incluso para ejecutar código no deseado.

Aunque no hay evidencia de que tu sitio esté actualmente infectado con malware, sí hay señales de que alguien ha estado intentando colarse. Por ejemplo, se han detectado más de 200 intentos de fuerza bruta en los últimos días, y más de mil intentos de escanear tu servidor en busca de archivos sensibles. Esto no es casualidad: es un ataque organizado. Y aunque tu CMS (WordPress) está actualizado, hay plugins y temas que no lo están, lo que aumenta el riesgo. Uno de esos plugins tiene una vulnerabilidad conocida con una puntuación de gravedad moderada, lo que significa que podría ser explotado si no se actualiza.

Lo más urgente es que tu sitio no está protegido de manera adecuada contra estos ataques. No tienes un firewall de capa 4 ni bloqueo automático de IPs maliciosas gestionado por el proveedor, y eso deja tu servidor expuesto. Afortunadamente, sí puedes activar una protección externa con Cloudflare, que actúa como una puerta de entrada segura y filtra gran parte del tráfico malicioso antes de que llegue a tu servidor. Eso es un primer paso crucial.

En resumen: tu web está en un estado de riesgo alto, pero con acciones concretas y rápidas, puedes recuperar el control y protegerla. No es un desastre, pero tampoco algo que puedas ignorar. Estamos aquí para ayudarte a resolverlo, paso a paso.

QUÉ HEMOS ENCONTRADO · POR GRAVEDAD

Análisis de SWPANEL.COM generado por SWPanel

Conclusiones

MEDIO

Errores críticos en el código del sitio

Se han encontrado 5 errores graves en 4 archivos distintos, incluyendo un agotamiento de memoria y accesos a propiedades nulas. Estos errores pueden causar caídas del sitio o permitir que los atacantes exploren vulnerabilidades.

ALTO

418 intentos

Ataques de fuerza bruta y escaneo agresivo

Se han detectado 418 intentos de adivinar contraseñas y 1312 intentos de acceder a archivos sensibles. Esto indica que alguien está intentando entrar o encontrar puntos débiles.

MEDIO

2 errores BD

Errores en la base de datos

Dos errores de base de datos muestran que hay consultas mal formadas o columnas inexistentes. Esto puede deberse a un código desactualizado o a intentos de inyección SQL.

ALTO

2 por actualizar

Plugins y temas desactualizados

Dos plugins o temas no están actualizados, y uno de ellos tiene una vulnerabilidad conocida. Esto aumenta el riesgo de que se aprovechen errores ya identificados.

MEDIO

Falta de protección activa

No se dispone de firewall de capa 4 ni bloqueo automático de IPs maliciosas gestionado por el proveedor. El sitio no tiene una capa de seguridad activa que filtre el tráfico malicioso.

PLAN DE ACCIÓN · PASOS A SEGUIR

1

Activar Cloudflare como CDN

URGENTE

Esto filtrará bots, IPs maliciosas y ataques antes de que lleguen a tu servidor. Puedes activarlo desde el panel de SWPanel sin necesidad de comandos ni configuraciones complejas.

2

Actualizar plugins y temas desactualizados

Revisa el panel de WordPress y actualiza los plugins y temas que no estén en la última versión. Uno de ellos tiene una vulnerabilidad conocida que debes corregir.

Análisis de SWPANEL.COM generado por SWPanel

Conclusiones

3

Revisar y corregir errores críticos en el código

Trabaja con un desarrollador para solucionar los errores de PHP, especialmente el de agotamiento de memoria y los accesos a propiedades nulas.

4

Configurar reglas de bloqueo manual

Aunque no tienes Fail2Ban gestionado, puedes usar iptables para bloquear IPs que hayan realizado múltiples intentos de ataque. Ejemplo:

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

5

Revisar permisos y seguridad de archivos

Asegúrate de que archivos sensibles como .env o wp-config.php.bak no estén accesibles públicamente. Puedes usar .htaccess para restringir el acceso:

```
<Files .env>
Order allow,deny
Deny from all
</Files>
```

Entiendo que esto puede parecer abrumador, pero no estás solo. Lo que hemos encontrado se puede resolver con acciones concretas y rápidas. Lo más urgente es activar una protección externa con Cloudflare y corregir los errores en el código. Una vez que tengas esas medidas en marcha, el riesgo disminuirá considerablemente. Si necesitas ayuda con cualquiera de estos pasos, estoy aquí para acompañarte. No es necesario que lo hagas todo de inmediato, pero sí que empieces por lo más urgente. Tu web puede recuperar su seguridad y estabilidad, y juntos lo lograremos.

Este es un informe Standard: cubre el estado de la web y de su código. No incluye la capa de inteligencia de seguridad (código malicioso en disco, red maliciosa, ataques priorizados y explotabilidad de CVE), disponible en el informe Premium.

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

7m 44s	6m 28s	1m 16s
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

2	5.051	2.120
LLAMADAS AL MODELO	TOKENS DE ENTRADA	TOKENS GENERADOS

7.171	~18 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