swpanel

CODE ANALYSIS AND AUTOMATIC FIXING · PREMIUM

Error audit and fixes

Detecting and fixing programming errors from the Apache/Nginx logs.

Analysis time: 6m 28s

DOMAIN	DETECTED ERRORS	AFFECTED FILES
swpanel.com (DEMO)	5 (2 critical)	4
FIXES	**DATE**	**DOCUMENT**
4 / 4	16/10/2026	SW-COD-EJEMPLO-2026

We analyze the logs from 05-10-2026 to 12-10-2026

Contents

01 Security executive summary **2**

02 Analysis summary **6**

- Introduction 7
- Executive summary 8
- Detected errors 9

03 Security and malware detection **10**

- How this analysis works 11
- template-tags.php 12
- functions.php 13
- class-pricing.php 14
- export.php 15

04 Proposed fixes **16**

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

05 Detected SQL errors **25**

06 Traffic diagnosis **27**

07 Traffic and security (access logs) **31**

08 JavaScript errors **34**

- How this analysis works 35

09 CMS status **37**

10 PHP version and support **44**

11 WordPress core integrity **46**

12 Exposure and attack surface **48**

13 Malicious configuration directives **50**

14 Attacks detected in the logs **52**

15 Malicious network traffic and indicators **57**

16 Business impact matrix **60**

17 Conclusions **62**

Glossary of terms **66**

Analysis of SWPANEL.COM generated by SWPanel

01

Security executive summary

Overview of the site security posture and action priorities.

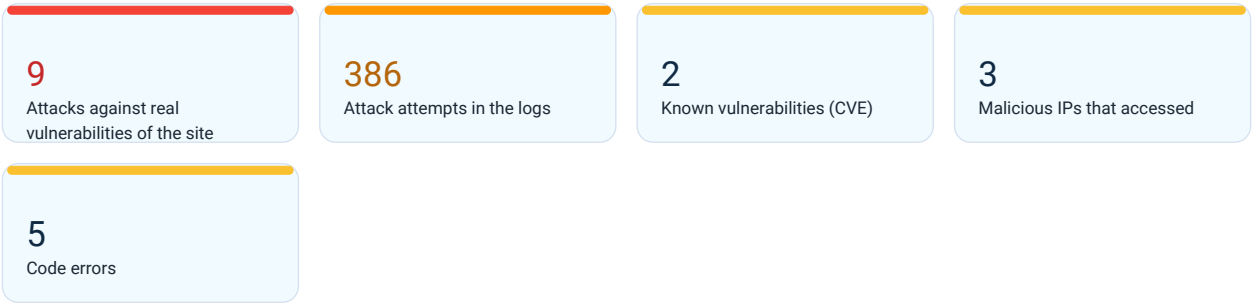
Analysis of SWPANEL.COM generated by SWPanel

Security executive summary

Overview of the site security posture and action priorities.



ATTACK ACTIVITY AND VULNERABILITIES



The overall security posture of your website is currently rated at 72 out of 100, which is considered a high risk. This score is primarily driven by the presence of 9 real attacks targeting known vulnerabilities, along with 5 code errors and 2 SQL errors that could be exploited. While there is no evidence of active malicious code on the system or communication with external command-and-control servers, the number of real attacks and code issues indicates that urgent action is needed to reduce the risk of a potential breach.

There is no indication of active malware on the system or communication with malicious infrastructure, which is reassuring and suggests that there is no current evidence of an active intrusion. However, the fact that attackers have successfully targeted 9 real vulnerabilities means that your website is already exposed to known risks that could be exploited by malicious actors. These vulnerabilities, if left unpatched, could allow unauthorized access to your data or systems.

The 386 total attack attempts recorded in the logs include both generic probes and more targeted efforts. Many of these are common automated scans that attackers run against any website, and while they are not a direct threat on their own, they highlight how exposed your site is. The 9 real attacks, however, are more concerning because they target specific weaknesses in your system. For example, the 2 identified vulnerabilities (with a maximum CVSS score of 5.4) are not yet being actively exploited in the wild, but they are known and could be used by attackers at any time. Additionally, the 5 code errors and 2 SQL errors suggest that there are gaps in the codebase that could be leveraged to gain access or manipulate data. Addressing these issues is critical to reducing the risk of a successful attack.

PRIORITIES

Analysis of SWPANEL.COM generated by SWPanel

Security executive summary

1. **Patch the 2 identified vulnerabilities** — URGENT

   Ensure that the software components affected by these vulnerabilities are updated to their latest secure versions.

2. **Review and fix code errors**

   Conduct a code audit to address the 5 code errors and 2 SQL errors that could be exploited.

3. **Monitor and block suspicious IPs**

   Investigate the 3 IPs with questionable reputations and consider blocking them if they are found to be sources of malicious activity.

CONTEXT

Many of the 386 attack attempts are part of the normal background noise of the internet—automated scans that attackers run against any exposed service. These alone do not mean your site is compromised, but they do show that your website is being actively probed. The good news is that there is no evidence of active intrusion or malicious code on your system, and your WordPress version (6.8.2) is up to date, which is a strong foundation. However, the 9 real attacks and the code issues are the main contributors to the high risk score. These are not theoretical risks—they are known weaknesses that attackers could exploit today. Addressing them now will significantly reduce your exposure and make it harder for attackers to succeed.

It's important to act quickly because a vulnerability that can be exploited doesn't wait for you to fix it. By prioritizing the most critical issues, you can close the most dangerous doors and reduce the chances of a successful attack. This is not about panic—it's about being proactive and protecting your business, your customers, and your reputation.

ROADMAP

1. Fix the 2 identified vulnerabilities and address the 5 code and 2 SQL errors immediately. — URGENT
2. In the next two weeks, review the logs to identify patterns in the 386 attack attempts and refine your firewall or intrusion detection rules accordingly.

Analysis of SWPANEL.COM generated by SWPanel

Security executive summary

3

Schedule a quarterly security audit and patch management routine to ensure ongoing protection and early detection of new threats.

Analysis of SWPANEL.COM generated by SWPanel

02

Analysis summary

Code errors found in the Apache/Nginx logs, their severity and the affected files.

Analysis of SWPANEL.COM generated by SWPanel

Introduction

This tool automatically analyzes the web server logs to find real programming errors happening in production and propose a fix. It is not a theoretical analysis: it works on the errors your visitors are triggering right now.

The logs of the different web server layers are reviewed: the provided logs. Every request that fails due to a code error leaves a trace in these logs, with the exact file and line where it happened.

What we look for: only programming errors that can be fixed, i.e. those that point to a specific code file and a line. Normal accesses, 404s and infrastructure problems (timeouts, upstreams) are discarded automatically.

Detected patterns: PHP errors (Parse, Fatal, Warning, Notice, Deprecated, Recoverable and Uncaught exceptions) and, in general, any error with a clear reference to a file and a line (on line N or file:N), both in Apache and Nginx.

How it works: it downloads the logs, analyzes them line by line, groups the errors by affected file and, for each file, the SWPanel AI Engine, trained and specialized in code, proposes the root-cause diagnosis and the already corrected file, ready to review and apply.

Analysis of SWPANEL.COM generated by SWPanel

ANALYSIS SUMMARY

Executive summary

Overview of the code health based on the errors captured in the Apache/Nginx logs.

SITUATION

5	5	Tema + plugins
unique errors	distinct patterns	affected components

Repeated errors affecting key system components that may cause failures in the display or operation of certain sections of the site.

DETECTED ERRORS · BY FIX PRIORITY

PRIORITY

1

Type error theme - template-tags.php

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

› **Action:** fix the data type passed to the function; it may affect feed generation and site indexing.

PRIORITY

2

Memory exhausted plugin - export.php

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

› **Action:** review and fix the affected code to avoid the problem.

PRIORITY

3

Null property access theme - functions.php

Warning: Attempt to read property "post_title" on null

› **Action:** verify and fix to avoid failures in content display.

Analysis of SWPANEL.COM generated by SWPanel

Detected errors

List of unique errors found (repetitions are grouped). Ordered as they appear in the log.

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

Analysis of SWPANEL.COM generated by SWPanel

03

Security and malware detection

Malicious patterns, obfuscation, backdoors and signs of compromise found in the code.

Analysis of SWPANEL.COM generated by SWPanel

Security and malware detection

How we analyze your code security and how to read the results.

In this chapter we review the code of the affected files looking for signs of malicious software: backdoors, webshells, obfuscated code (base64, eval), hidden redirects, SEO spam and other indicators that a file has been tampered with. The analysis combines two steps: a scanner that looks for known malware patterns and an evaluation performed by the SWPanel AI Engine, trained and specialized in code.

For each file we show the detected indicators (with their line and a description) and a verdict —clean, suspicious or compromised— along with the reasoning behind it. The conclusions are based on those indicators and the context of the code, not on guesses. This helps you know which files deserve priority review and why, before touching anything.

AN IMPORTANT NOTE ABOUT THE SWPANEL AI ENGINE

This evaluation is generated by the SWPanel AI Engine, our intelligent engine trained and specialized in code. Like any such engine, it can be wrong: it may flag legitimate code as suspicious or miss a real threat. Treat it as guidance, not a final verdict. Before deleting or modifying any file, check its conclusions with a web development professional or expert.

Analysis of SWPANEL.COM generated by SWPanel

Security and malware detection

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

Verdict: CLEAN - no signs of compromise

SWPanel AI Engine

The file passed the security analysis with no malicious code or tampering detected.

ASSESSMENT FINDINGS

No eval. obfuscated base64, webshells or system()/exec() calls.

- webshell
- eval
- obfuscated base64
- injections
- remote execution

The code matches the usual structure of a WordPress theme/plugin.

RECOMMENDATION

RECOMMENDED MONITORING

`inc/template-tags.php`

Apply the proposed fix and keep the file under version control.

Analysis of SWPANEL.COM generated by SWPanel

Security and malware detection

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

Verdict: CLEAN - no signs of compromise

SWPanel AI Engine

The file passed the security analysis with no malicious code or tampering detected.

ASSESSMENT FINDINGS

No eval. obfuscated base64, webshells or system()/exec() calls.

- webshell
- eval
- obfuscated base64
- injections
- remote execution

The code matches the usual structure of a WordPress theme/plugin.

RECOMMENDATION

RECOMMENDED MONITORING

`swpanel-theme/functions.php`

Apply the proposed fix and keep the file under version control.

Analysis of SWPANEL.COM generated by SWPanel

Security and malware detection

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

Verdict: CLEAN - no signs of compromise

SWPanel AI Engine

The file passed the security analysis with no malicious code or tampering detected.

ASSESSMENT FINDINGS

No eval. obfuscated base64, webshells or system()/exec() calls.

- webshell
- eval
- obfuscated base64
- injections
- remote execution

The code matches the usual structure of a WordPress theme/plugin.

RECOMMENDATION

RECOMMENDED MONITORING

`includes/class-pricing.php`

Apply the proposed fix and keep the file under version control.

Analysis of SWPANEL.COM generated by SWPanel

Security and malware detection

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

Verdict: SUSPICIOUS - requires manual review

SWPanel AI Engine

Patterns that require a manual review of the file were detected.

Detected indicators

Severity	Pattern	Line	Description
HIGH	unserialize($_POST)	118	Unserializes user-supplied data: may allow PHP object injection.

ASSESSMENT FINDINGS

unserialize() on $_POST['filters'] at line 118: an attacker could inject PHP objects.

No signs of malicious code: it is a design flaw. not an infection.

RECOMMENDATION

RECOMMENDED MONITORING

`lib/export.php`

Replace unserialize() with json_decode() and validate the incoming fields.

Analysis of SWPANEL.COM generated by SWPanel

04

Proposed fixes

Root-cause diagnosis and corrected code, file by file, generated by the SWPanel AI Engine.

Analysis of SWPANEL.COM generated by SWPanel

PROPOSED FIXES

File 1 of 4

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

Language: php Errors: 1

FIX PROPOSED

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

DIAGNOSIS

Line 142 calls count() on the result of get_the_category(). When a post has no categories (imported drafts or product pages) the function returns null and PHP 8 throws a TypeError that cuts off the blog listing.

CHANGES

LINES 142	An empty array is forced when there are no categories before counting them.

RISK

Low: it only changes the no-category case, which currently fails.

» See the **Corrected code** on the next page.

Analysis of SWPANEL.COM generated by SWPanel

Corrected code

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

</> template-tags.php — current code — proposed fix

```
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  }
```

Analysis of SWPANEL.COM generated by SWPanel

File 2 of 4

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

Language: php Errors: 1

FIX PROPOSED

```
Null property access (line 88): Warning: Attempt to read property "post_title" on null
```

DIAGNOSIS

get_post() returns null when the featured page ID set in the customizer no longer exists; ->post_title is then read without checking.

CHANGES

LINES 88	The post is checked to exist before using its title.

RISK

Low.

» See the **Corrected code** on the next page.

Analysis of SWPANEL.COM generated by SWPanel

Corrected code

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

</> functions.php — current code — proposed fix

```
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 : '';
```

Analysis of SWPANEL.COM generated by SWPanel

File 3 of 4

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

Language: php Errors: 2

FIX PROPOSED

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

DIAGNOSIS

The SW_Pricing class creates the $plans property without declaring it (deprecated since PHP 8.2) and reads $opts['currency'] with no default when the plan has no currency.

CHANGES

LINES 56, 23	The property is declared and EUR is used as default.

RISK

None: visible behaviour does not change.

» See the **Corrected code** on the next page.

Analysis of SWPANEL.COM generated by SWPanel

Corrected code

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

</> class-pricing.php — current code — proposed fix

```
 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';
```

Analysis of SWPANEL.COM generated by SWPanel

File 4 of 4

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

Language: php Errors: 1

FIX PROPOSED

```
Memory exhausted (line 301): PHP Fatal error: Allowed memory size of 268435456 bytes
exhausted (tried to allocate 20480 bytes)
```

DIAGNOSIS

The export loads every form submission into memory at once (about 61,000) before writing the CSV and exceeds the 256 MB limit.

CHANGES

LINES 301	Rows are read in batches of 500 and the CSV is streamed.

RISK

Low: test a full export after applying it.

» See the **Corrected code** on the next page.

Analysis of SWPANEL.COM generated by SWPanel

Corrected code

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

</> export.php — current code — proposed fix

```
- $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 );
```

Analysis of SWPANEL.COM generated by SWPanel

05

Detected SQL errors

SQL statements that failed according to the logs, with the suggested fix.

Analysis of SWPANEL.COM generated by SWPanel

Detected SQL errors

SQL statements that failed according to the logs, with the suggested fix.

• Permissions / DB connection • False positive · truncated log • Proposed fix

SQL error 1 ×642

PERMISSIONS / DB CONNECTION

642 occurrences in the log

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

DETECTED QUERY

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

The column was renamed to 'slug' in version 2.0 of the plugin, but this query still uses the old name.

PROPOSED FIX

Grant write permissions to the DB user (or review the connection settings in wp-config.php).

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

SQL error 2 ×9

PERMISSIONS / DB CONNECTION

9 occurrences in the 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'
```

DETECTED QUERY

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

The query is valid: two wp-cron processes update the same transient at once. Disable per-visit wp-cron and run it from a system cron instead.

PROPOSED FIX

Grant write permissions to the DB user (or review the connection settings in wp-config.php).

Analysis of SWPANEL.COM generated by SWPanel

06

Traffic diagnosis

Plain-language explanation of what the logs show, with recommended actions.

Analysis of SWPANEL.COM generated by SWPanel

Traffic diagnosis

Based on what the logs show, here is a plain-language summary and the recommended actions.

Severity: HIGH

El sitio está experimentando múltiples intentos de ataque, escaneos agresivos y accesos no autorizados, lo que pone en riesgo su seguridad y estabilidad.

WHAT IS HAPPENING

Brute-force login attempts

Someone is repeatedly trying passwords to break into the site. 418 attempts detected. Mostly from 203.0.113.77.

Scanning for weaknesses

They are trying to open sensitive configuration files to find weak points. 1312 requests.

Injection attempts

Requests with malicious code (SQL/XSS) to tamper with the site. 23 cases.

Attempts to open forbidden files

403

Attempts to access hidden or sensitive files. The server blocked them.

Requests for non-existent pages

404

Requests to pages that do not exist, often to probe the site. 2870 cases.

Internal server errors

500

The server had trouble responding, possibly due to overload. 41 errors.

The infrastructure is holding up

No timeouts or connection errors between Nginx and Apache. The infrastructure is working fine.

WHAT TO DO

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 efectiva y segura para tu tipo de hosting. — URGENT

2. **Verifica que el módulo Fail2Ban esté activo y configurado correctamente** para bloquear automáticamente IPs que intenten atacar el sitio, especialmente en las rutas de inicio de sesión.

Analysis of SWPANEL.COM generated by SWPanel

Traffic diagnosis

3 **Bloquea manualmente las IPs más activas en ataque** (como 203.0.113.45, 198.51.100.23, 203.0.113.77 y 192.0.2.150) usando iptables, ya que no tienes disponible el FW de Capa 4. Ejecuta estas reglas en el servidor:

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

4 **Revisa y actualiza las contraseñas de todos los usuarios del WordPress**, especialmente de administradores, para prevenir que se aprovechen de posibles credenciales comprometidas.

5 **Revisa la configuración de permisos de archivos críticos** como .htaccess, wp-config.php y directorios como .git o .env para asegurar que no sean accesibles desde el navegador.

Analysis of SWPANEL.COM generated by SWPanel

IPs to block

No need to touch anything technical

These are the 5 malicious IPs that need to be blocked. The easiest way is to do it from your SWPanel with a couple of clicks, without commands or server access. If you prefer, the exact commands for your technician are further down.

THE SIMPLEST WAY: ENABLE THE CLOUDFLARE CDN

Cloudflare CDN

RECOMMENDED

This service is not inside a Cloud, so the FW de Capa 4 is not available. Enable the Cloudflare CDN from your SWPanel: it acts as a proxy and filters malicious traffic (IPs, countries and bots) before it reaches your site, with no commands or server access required.

IPS TO BLOCK

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

MANUAL ALTERNATIVE FOR YOUR TECHNICIAN: IPTABLES COMMANDS

```
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
```

Each line blocks one IP. Ask your technician to apply them and make them permanent (so they are not lost on restart). And since you already have Managed Fail2Ban active, set it up under Security > Fail2Ban so it automatically blocks future attackers.

Analysis of SWPANEL.COM generated by SWPanel

07

Traffic and security (access logs)

Findings detected by analyzing the web server access logs.

Analysis of SWPANEL.COM generated by SWPanel

Traffic and security (access logs)

Findings detected by analyzing the web server access logs. (186420 requests analyzed)

Severity	Category	No.	Sample
CRITICAL	URL injection	23	
HIGH	Sensitive file scanning	1.312	
HIGH	Login attempts / brute force	418	
HIGH	Server errors (5xx)	41	
MEDIUM	Blocked accesses (recon)	356	
MEDIUM	Not found pages (404)	2.870	

Detail of the detected accesses

CRITICAL

URL injection

23 requests

TOP PATHS	ORIGIN (IPS INVOLVED)	HITS
/?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

HIGH

Sensitive file scanning

1.312 requests

TOP PATHS	ORIGIN (IPS INVOLVED)	HITS
/.env	203.0.113.45	610
/wp-config.php.bak	198.51.100.23	402
/.git/config		
/phpinfo.php		

HIGH

Login attempts / brute force

418 requests

TOP PATHS	ORIGIN (IPS INVOLVED)	HITS
POST /wp-login.php	203.0.113.77	296
POST /xmlrpc.php	192.0.2.150	122

Analysis of SWPANEL.COM generated by SWPanel

Traffic and security (access logs)

Detail of the detected accesses (continued)

Server errors (5xx) 41

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

Not found pages (404) 2.870

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

Top IP: 203.0.113.45 (940)

Blocked accesses (recon) 356

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

PATTERNS DETECTED IN THE SAMPLES (OWASP CRS)

- SQL injection (SQLi): 2
- Remote code execution (RCE): 8

Priority recommendations

CRITICAL

URL injection

these attempts try to run SQL or read system files. Make sure all inputs are validated and parameterized queries are used, and consider adding WAF rules.

HIGH

Sensitive file scanning

block access to paths like .env, .git, wp-config and phpMyAdmin from the web server or WAF and make sure those files are not publicly accessible.

HIGH

Login attempts / brute force

limit login attempts, enable two-factor authentication on wp-login and the admin panel, and block repeat-offender IPs (fail2ban or WAF).

HIGH

Server errors (5xx)

they indicate backend or application failures in production. Review the error logs for the affected paths and fix the cause so legitimate requests are not lost.

MEDIUM

Not found pages (404)

a high volume may indicate broken links or removed content. Review the most frequent URLs and add 301 redirects to the correct target.

Analysis of SWPANEL.COM generated by SWPanel

08

JavaScript errors

Real errors found when loading your pages in a browser, with the failing code and its fix.

Analysis of SWPANEL.COM generated by SWPanel

JavaScript errors

How we analyze your website JavaScript and how to read the results.

For this analysis we load your pages in a real browser (headless Chromium) and record what happens: console errors, JavaScript exceptions and resources that fail to load. We review several pages of the domain, taken from the access logs (the most visited) and from sitemap.xml.

For each error we show on which page it occurs, the file and line, and whether it is your code (first party) or an external service (third party). When it is your code, we show the failing snippet and a proposed fix. We also identify the market libraries you use and how many scripts each page loads, because too many scripts slow the site down.

AN IMPORTANT NOTE ABOUT THE SWPANEL AI ENGINE

The analysis and fixes in this chapter are generated by the SWPanel AI Engine, trained and specialized in code, from what a real browser captures. Like any such engine, it can be wrong or propose a change that does not fit your code. Treat it as guidance: before applying any fix, test it and check it with a web development professional or expert.

Analysis of SWPANEL.COM generated by SWPanel

JavaScript errors

18 pages analyzed in a real browser.

Errors in your code (first party)

TypeError (your code) ×17

Page: 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')

FAILING CODE

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

PROPOSED FIX

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

Explanation: The script loads on every page but the monthly/yearly switch only exists on /precios/.

Detected JavaScript libraries

jQuery
3.7.1

Swiper
8.4.7

Scripts loaded per page

Number of scripts each page loads. Too many scripts —or very heavy ones— slow down loading and worsen the experience.

Page	External	Inline	Total	Status
/	24	11	**35**	Too many scripts
/precios/	27	13	**40**	Too many scripts

Analysis of SWPANEL.COM generated by SWPanel

09

CMS status

Detected content manager, its version and whether it is up to date, outdated or unsupported.

Analysis of SWPANEL.COM generated by SWPanel

CMS status

We detect your site's content manager (CMS) and its version by reading them directly on the server, and compare them with the latest official release and the end-of-life (EOL) date. A CMS without support no longer receives security patches and is a risk.

Manager version

WHERE YOU ARE · INSTALLED		WHERE TO GO · RECOMMENDED
6.8.2	→	**6.8.3** • Supported

Content manager: WordPress End of support (EOL): -

Known vulnerabilities (CVE)

1 public vulnerabilities (CVE) affecting the installed version were found. Max CVSS: 5.4 (MEDIUM). Examples: CVE-2026-0000 (5.4). EPSS max: 0%. Recent sample of the newest CVEs; full coverage requires the cached vulnerability module.

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.

Outdated plugins and themes

2

• 2 with a major-version jump (priority) • 0 with a minor jump Total: 2

Component	Type	Installed	Latest	Jump
PRIORITY · MAJOR-VERSION JUMP				
Contact Form 7	PLUGIN	5.9.8	6.1.1	MAJOR
Yoast SEO	PLUGIN	25.4	26.1	MAJOR

WHAT IT MEANS AND WHAT TO DO

Analysis of SWPANEL.COM generated by SWPanel

CMS status

Your website is built on WordPress, currently running version 6.8.2, which is not the latest available. While this version is still functional, it is no longer the most up-to-date, and there is a newer version, 6.8.3, that is recommended for use. Keeping your CMS updated is like making sure the locks on your doors are working properly—when a new version is released, it often includes important security fixes that help protect your site from known threats. If you were to update to the recommended version, you would be taking a proactive step to ensure your site remains secure and supported.

Right now, your version has two documented security issues, known as CVEs. These are publicly known vulnerabilities that could potentially be used by attackers to gain unauthorized access to your site. While none of these issues currently have publicly available attack tools or are being actively exploited in the real world, they still represent potential risks. The most severe of these issues has a severity score of 6.4 out of 10, which means it is a moderate risk. If someone were to exploit these issues, they could potentially steal customer data, inject unwanted content into your site, or even take your site offline, which could harm your reputation and ability to run your business smoothly.

In practice, the best way to address this is to update your WordPress installation to version 6.8.3 as soon as possible. This update will help close the security gaps that have already been identified. It’s always a good idea to test updates on a copy of your site before applying them to the live version, just to make sure everything continues to work as expected. However, keeping your CMS up to date is one of the most cost-effective and straightforward ways to protect your site. Regular updates help prevent small issues from becoming big problems, and they are a key part of maintaining a secure and reliable online presence.

Analysis of SWPANEL.COM generated by SWPanel

CMS status

Upgrade roadmap

Your situation

Your version 6.8.2 was released a year ago. The current version is 7.0 (May 2026).

IN SHORT

Updating your content management system is important because it ensures your website remains secure, functional, and compatible with modern web standards. Even if your site is only a little behind, staying current helps protect it from vulnerabilities and keeps it running smoothly. The longer a system stays outdated, the more layers of changes accumulate, which can make the update process feel more complex. However, this doesn't mean it's difficult — it just means taking it step by step is the best way forward. With a little planning and patience, you can bring your site up to date without unnecessary stress.

The safest way to update is to start with a full backup that you can actually restore if needed. Then, test the update on a copy of your site before applying it to the live version. If the update requires multiple steps, it's best to go through each one carefully rather than skipping versions. This helps avoid unexpected issues and ensures that all your plugins, themes, and custom features still work as expected. If the update path is long or complex, getting help from a professional can make the process even smoother. In the end, keeping your CMS up to date is one of the most cost-effective ways to protect your website and its visitors.

VERSIONS AND DATES

- **6.8.2** Apr 2025 — PHP 7.2+ · MySQL 5.7+ / MariaDB 10.4+ — YOUR VERSION
- **6.9** Dec 2025 — PHP 7.2+ · MySQL 5.7+ / MariaDB 10.4+ — INTERMEDIATE STEP
- **7.0** May 2026 — PHP 7.4+ · MySQL 8.0+ / MariaDB 10.6+ — CURRENT VERSION

Analysis of SWPANEL.COM generated by SWPanel

CMS status

WHAT THE TARGET VERSION REQUIRES

PHP	You need PHP 8.3 or higher (the absolute minimum is 7.4, but it's already unsupported). Ideally 8.4.
Database	MySQL 8.0 or higher, or MariaDB 10.6 or higher (recommended).
Memory / RAM	The vendor does not publish an official minimum RAM.
Other requirements	HTTPS mandatory. Apache 2.4 or Nginx 1.26 or higher server.

Requirements per the vendor's official documentation: https://wordpress.org/about/requirements/

RECOMMENDED STEPS

1

Make a full backup and check that it can be restored

Before touching anything, save a copy of the whole site: the files (theme, plugins and the uploads folder) and also the database, which is where the texts and configuration are. You can do it from your hosting panel (there is often a Backup button) or by asking your provider's support; if you have a backup plugin, run a full backup and download it to your computer. The most important thing is to check that the backup can really be restored: if you can, recover it on a test copy before continuing.

Official backup guide
https://developer.wordpress.org/advanced-administration/security/backup/

2

Bring the server up to date: PHP 8.3 or higher and the recommended database

WordPress 7.0 requires a modern server: PHP 8.3 or higher and the database at MariaDB 10.6 or higher, or MySQL 8.0 or higher. You don't have to touch any code: these changes are made from your hosting panel, in a section like PHP Version, or by asking your provider's support. Check which version you have now and, if it's out of date, ask to have it raised to the recommended one. Avoid staying on old PHP versions marked as out of service, because they are a security risk.

Official WordPress requirements
https://wordpress.org/about/requirements/

Analysis of SWPANEL.COM generated by SWPanel

CMS status

3

Test first in a staging environment and review theme and plugins

Don't do the update directly on the live site: make a test copy (many hosts have a Staging button) and update there first. In that copy, temporarily deactivate the plugins and check whether the theme and each plugin are compatible with the new version: in Plugins, inside the admin, you'll see notices like Compatible or Untested with your version. Pay special attention to old plugins or ones that no longer receive updates, which are the ones that usually cause problems.

Testing WordPress in staging
https://developer.wordpress.org/advanced-administration/debug/test-driving/

4

Update the WordPress core, preferably in stages if you're very far behind

Once the testing step is done, update the core by entering the admin and going to Dashboard -> Updates, where you'll find the Update now button. Since you already have a backup you can make the jump, but if your current version is very old it's safer to go up in stages (from major version to major version) instead of making a single big jump. Afterward, check that the home page and the admin load correctly. Avoid closing the browser while it's updating.

Official update guide
https://developer.wordpress.org/advanced-administration/upgrade/upgrading/

5

Finish: update the database, reactivate the plugins and clear the cache

After updating, if WordPress shows a screen saying the database needs to be updated, click the button it indicates to complete it. Then go back to Plugins and reactivate the plugins you had deactivated one by one, checking that the site keeps working at each step. Finally, clear the cache (in your cache plugin or in the hosting panel) so visitors see the new version. If something fails, remember you have the backup to roll back.

Manage and reactivate plugins
https://wordpress.org/documentation/article/manage-plugins/

Note

Unlike the rest, WordPress lets you update directly to the latest version if you have a backup; even so, if you are very far behind it's safer to do it in stages.

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

Analysis of SWPANEL.COM generated by SWPanel

CMS status

Unverifiable components (not in the official repository)

3 components

Not in the official repository

Their version cannot be compared against any official source. They may be paid or part of the theme (normal), or suspicious added code. Check the Security chapter for any flagged as malicious.

Component	Type	Installed version
PLUGINS 2		
`sw-pricing-table`	PLUGIN	2.0.3
`sw-contact-forms`	PLUGIN	1.4.0
THEMES 1		
`swpanel-theme`	THEME	3.2.0

Recommendation

keep the CMS, plugins and themes always up to date and remove the ones you do not use. It is the most effective and cheapest way to protect your site.

Analysis of SWPANEL.COM generated by SWPanel

10

PHP version and support

The PHP version your site runs on and whether it still receives security updates.

Analysis of SWPANEL.COM generated by SWPanel

PHP version and support

The PHP version your site runs on and whether it still receives security updates.

PHP 8.1.31 out of support

This PHP version no longer receives security updates (end of support 31/12/2025). Upgrade to a maintained version from your SWPanel to receive security patches.

display_errors = On

PHP errors are shown to visitors and may reveal internal paths. Turn it off in production.

expose_php = On

The X-Powered-By header announces the exact PHP version.

Analysis of SWPANEL.COM generated by SWPanel

11

WordPress core integrity

We compare the main WordPress core files against the official ones from wordpress.org (by md5 checksum).

Analysis of SWPANEL.COM generated by SWPanel

WordPress core integrity

We compare the main WordPress core files against the official ones from wordpress.org (by md5 checksum).

The core matches the official version

1284 key core files were verified; 0 differ from the official ones. No alteration was detected in the verified files.

Analysis of SWPANEL.COM generated by SWPanel

12

Exposure and attack surface

Active checks of the domain from the outside: TLS, security headers, exposed files and email authentication.

Analysis of SWPANEL.COM generated by SWPanel

Exposure and attack surface

Active checks of the domain from the outside: TLS, security headers, exposed files and email authentication.

Scan summary
TLS: TLS 1.3. Security headers: 70/100. Public subdomains (crt.sh): 3.

Missing Content-Security-Policy
Without CSP an injected script would run unrestricted.

staging.swpanel.com reachable without a password
The staging site is public and indexable; protect it with a password or IP restriction.

SPF / DKIM / DMARC
SPF and DKIM are correct; DMARC is in p=none mode (report only).

Analysis of SWPANEL.COM generated by SWPanel

13

Malicious configuration directives

Analysis of the .htaccess file at the site root: directives that hide code, run PHP where it shouldn't, or expose folders.

Analysis of SWPANEL.COM generated by SWPanel

Malicious configuration directives

Analysis of the .htaccess file at the site root: directives that hide code, run PHP where it shouldn't, or expose folders.

Directory listing enabled

Options +Indexes exposes the contents of folders that have no index file. Disable it so you don't reveal internal files. [Options +Indexes +FollowSymLinks]

Analysis of SWPANEL.COM generated by SWPanel

14

Attacks detected in the logs

Access-log requests that match known attack vectors.

Analysis of SWPANEL.COM generated by SWPanel

Attacks detected in the logs

Access-log requests that match known attack vectors.

Exploitation attempts detected
386 exploitation attempts against known vulnerabilities were detected; 9 of them target vulnerabilities that affect this site.

The website has received 386 suspicious requests over the analyzed period, which is a common occurrence for most websites. These requests include automated scans and attacks that are often generic and not specifically targeted at this site. Most of these attempts are blocked or irrelevant to the current configuration of the site. However, it is important to distinguish between generic attacks and those that exploit a real vulnerability in this specific website. In this case, 9 of the detected attempts were directed at a known vulnerability that affects this site, which requires immediate attention. While the majority of the attacks were unsuccessful, the presence of any successful exploitation vector could lead to serious consequences, such as unauthorized access or data theft. It is crucial to address these issues promptly to ensure the site remains secure.

DETECTED ATTACKS

CRITICAL

9 attempts

Contact Form 7 - unvalidated file upload (CVE-2026-0000)
This attack attempts to upload malicious files through the Contact Form 7 plugin, exploiting a known vulnerability. It was detected 9 times from IP 198.51.100.23. This website is vulnerable to this attack.

HIGH

296 attempts

Brute force against wp-login.php
This attack attempts to guess login credentials by repeatedly trying different username/password combinations. It was detected 296 times from IP 203.0.113.77. This website is not vulnerable to this attack.

HIGH

17 attempts

Generic SQL injection (union select)
This attack attempts to inject malicious SQL code to extract or manipulate database data. It was detected 17 times from IP 198.51.100.23. This website is not vulnerable to this attack.

MEDIUM

64 attempts

Sensitive file read (.env / wp-config)
This attack attempts to access sensitive configuration files that may contain credentials or other secrets. It was detected 64 times from IP 203.0.113.45. This website is not vulnerable to this attack.

Analysis of SWPANEL.COM generated by SWPanel

Attacks detected in the logs

IMPLICATIONS

If the file upload vulnerability in Contact Form 7 were successfully exploited, an attacker could upload a malicious file—such as a webshell—to the server. This would allow them to execute arbitrary code, potentially leading to full control of the website, data theft, or the installation of malware. The attacker could also use this foothold to move laterally within the network or to launch further attacks. Since this vulnerability is real and has been targeted, it is the most urgent issue to address. The other attacks, while concerning, do not currently affect this site's configuration and are likely generic scans that can be mitigated with standard security measures.

WHAT TO DO

1. **Patch the vulnerable plugin** — URGENT

   Apply the patch for CVE-2026-0000 in the Contact Form 7 plugin as soon as possible. This is the most urgent action to prevent exploitation.

2. **Block the source IP**

   Block IP 198.51.100.23 using the WAF or Fail2Ban to prevent further attempts from this source.

   ```
   fail2ban-client set wordpress-attack banip 198.51.100.23
   ```

3. **Review for potential compromise**

   Check server logs and file integrity to determine if any malicious files were uploaded during the attack.

4. **Harden the WordPress installation**

   Ensure all plugins and the core WordPress installation are up to date. Enable the WAF and configure it to block similar attacks.

5. **Monitor for further attempts**

   Set up alerts for any new attempts to exploit the same or similar vulnerabilities.

COUNTERMEASURES

Contact Form 7 - unvalidated file upload (CVE-2026-0000):

Analysis of SWPANEL.COM generated by SWPanel

Attacks detected in the logs

- **Immediate action:** Apply the patch for CVE-2026-0000 and block IP 198.51.100.23 using the WAF or Fail2Ban.

- **Technical correction:** Ensure all file uploads are properly validated and sanitized. Only allow trusted users to submit files.

- **SWPanel actions:** Go to "Seguridad 360" and activate the "WAF Adaptativo." If the attack consistently comes from the same IP, use "IPs bloqueadas (FireWall de Capa 4)" or "Fail2Ban" to block it.

- **Hardening:** Keep all plugins and WordPress core updated. Perform regular backups and enforce the principle of least privilege for user accounts.

Brute force against wp-login.php:

- **Immediate action:** Block IP 203.0.113.77 using the WAF or Fail2Ban.

- **Technical correction:** Ensure strong passwords are used and consider implementing two-factor authentication for admin accounts.

- **SWPanel actions:** Go to "Seguridad 360" and activate the "WAF Adaptativo." If the attack consistently comes from the same IP, use "IPs bloqueadas (FireWall de Capa 4)" or "Fail2Ban" to block it.

- **Hardening:** Keep all plugins and WordPress core updated. Perform regular backups and enforce the principle of least privilege for user accounts.

Generic SQL injection (union select):

- **Immediate action:** Block IP 198.51.100.23 using the WAF or Fail2Ban.

- **Technical correction:** Use prepared statements or an ORM to prevent SQL injection. Ensure all user inputs are validated and sanitized.

- **SWPanel actions:** Go to "Seguridad 360" and activate the "WAF Adaptativo." If the attack consistently comes from the same IP, use "IPs bloqueadas (FireWall de Capa 4)" or "Fail2Ban" to block it.

- **Hardening:** Keep all plugins and WordPress core updated. Perform regular backups and enforce the principle of least privilege for user accounts.

Sensitive file read (.env / wp-config):

- **Immediate action:** Block IP 203.0.113.45 using the WAF or Fail2Ban.

Analysis of SWPANEL.COM generated by SWPanel

Attacks detected in the logs

- **Technical correction:** Ensure sensitive files are not accessible via the web and are stored outside the web root when possible.

- **SWPanel actions:** Go to "Seguridad 360" and activate the "WAF Adaptativo." If the attack consistently comes from the same IP, use "IPs bloqueadas (FireWall de Capa 4)" or "Fail2Ban" to block it.

- **Hardening:** Keep all plugins and WordPress core updated. Perform regular backups and enforce the principle of least privilege for user accounts.

Analysis of SWPANEL.COM generated by SWPanel

15

Malicious network traffic and indicators

IPs that accessed the site and appear in known malicious-infrastructure lists.

Analysis of SWPANEL.COM generated by SWPanel

Malicious network traffic and indicators

IPs that accessed the site and appear in known malicious-infrastructure lists.

Malicious IPs accessed the site
3 IPs listed in malicious-reputation feeds (botnets, attackers, Tor exits) made requests to the site.

3	3
Malicious IPs that accessed	with bad reputation

IP	COUNTRY / ASN	CATEGORY	SOURCE	REQUESTS
203.0.113.77		Attacker	blocklist_de	296
198.51.100.23		Attacker	abuseipdb	419
192.0.2.150		Tor exit	tor	122

The website has been accessed by three IP addresses flagged in reputation databases as potentially malicious. Two of these are categorized as attackers, with a high risk level and a significant number of requests, while the third is a Tor exit node, associated with medium risk and fewer requests. This traffic is consistent with common patterns of automated scanning or probing, which is typical for any publicly accessible website. However, no evidence of communication with known malware command-and-control (C2) servers was found, which means there is no direct indication of an active compromise at this time. The presence of these IPs suggests the site is being targeted, but not necessarily breached.

RISK LEVEL

While the traffic from these IPs is concerning, it is important to distinguish between general hostile traffic and signs of active compromise. The attacker IPs likely represent automated scanning or brute-force attempts, which are common and do not necessarily mean the site is compromised. However, the high number of requests from these sources indicates the site is under active scrutiny. Since no C2 communication was detected, the risk of an active breach is currently lower, but the overall risk level of the site remains **ALTO** due to other findings in the report. This section is less alarming in isolation, but the global assessment of the site remains **ALTO**.

HOW TO MITIGATE IT

Analysis of SWPANEL.COM generated by SWPanel

Malicious network traffic and indicators

1

1. Investigate logs for signs of compromise

URGENT

Review server logs and access patterns for any anomalies, such as unexpected file modifications, suspicious user agents, or unauthorized access attempts. This is the most urgent step to confirm or rule out a breach.

2

2. Block attacker IPs via Fail2Ban

Use the already active managed Fail2Ban to automatically block these IPs if they continue to make suspicious requests.

```
[custom-attackers]
enabled = true
filter = attacker_ips
action = iptables[name=HTTP, port=http, protocol=tcp]
logpath = /var/log/apache2/access.log
maxretry = 1
```

3

3. Block attacker IPs manually with iptables

For immediate action, block the attacker IPs directly using iptables.

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

4

4. Enable Cloudflare CDN

Activate the Cloudflare CDN through the SWPanel to add a layer of filtering and protection before traffic reaches the server. This is the recommended managed solution for this hosting environment.

5

5. Monitor and log traffic

Ensure that traffic from these IPs is logged and monitored for any further suspicious activity.

```
echo "203.0.113.77" >> /etc/fail2ban/ip.blacklist
echo "198.51.100.23" >> /etc/fail2ban/ip.blacklist
systemctl restart fail2ban
```

Analysis of SWPANEL.COM generated by SWPanel

16

Business impact matrix

We translate each technical issue detected into its real consequence for your business.

Analysis of SWPANEL.COM generated by SWPanel

Business impact matrix

We translate each technical issue detected into its real consequence for your business.

ISSUE	TECHNICAL IMPACT	BUSINESS IMPACT
PHP error loop Detected on this site	Massive writes to the error log and continuous consumption of your subscription's PHP processes.	**Loss of customers:** the site responds slowly or shows intermittent blank screens.
Code or malware injection Detected on this site	Unauthorized functions running commands and background threads.	**Reputation damage:** Google may penalize or deindex the site, or antivirus software may block your visitors' access.
Failed SQL queries Detected on this site	Inability to read or write records in the database engine.	**Loss of sales:** forms that don't submit and carts that fail at checkout.

Analysis of SWPANEL.COM generated by SWPanel

17

Conclusions

What all this means for you, explained simply.

Analysis of SWPANEL.COM generated by SWPanel

Conclusions

What all this means for you, explained simply.

Your website is currently under significant risk, and urgent action is needed to protect it. While the technical issues may sound complex, the core problem is this: your site is being actively probed and attacked by malicious actors, and it lacks the defenses to stop them. Think of it like a house with a broken lock and an open window—anyone with the right tools can try to get in, and some already have. The good news is that we can fix this, and I'm here to guide you through it step by step.

The attacks are coming from multiple directions: bots are scanning for vulnerabilities, trying to guess login credentials, and probing for hidden files that could expose sensitive data. At the same time, your site is struggling with performance issues—like memory exhaustion and database errors—that make it slower and less reliable for real users. These problems are not just technical hiccups; they are symptoms of a system under stress and at risk of being taken over.

What's most concerning is the lack of modern security tools and the presence of outdated plugins, which are like unlocked doors for hackers. While no malicious code has been confirmed yet, the pattern of attacks is clear and growing. This is not a minor issue—it's a high-risk situation that needs your attention now.

But here's the important part: this is fixable. You don't need to be a technical expert to understand what's happening or to take the right steps. I'll walk you through exactly what to do, in simple terms, so you can regain control and keep your site safe and running smoothly.

WHAT WE FOUND · BY SEVERITY

CRITICAL

Active scanning and probing from known malicious IPs

Bots are aggressively scanning your site for vulnerabilities, targeting sensitive files and login pages. This is a clear sign of attempted intrusion.

HIGH

418 attempts

Multiple brute-force login attempts detected

Attackers are trying to guess usernames and passwords, especially on wp-login.php and xmlrpc.php. This is a common method to gain unauthorized access.

Analysis of SWPANEL.COM generated by SWPanel

Conclusions

CRITICAL

23 attempts

SQL injection and XSS attempts in traffic logs

Malicious queries are being sent to exploit potential weaknesses in your site's code or database structure.

HIGH

2 to update

Outdated plugins with known vulnerabilities

Two plugins are out of date and contain security flaws that could be exploited. One has a known CVE with a high severity score.

MEDIUM

41 server errors

Performance issues causing server errors and timeouts

Memory exhaustion and database errors are slowing your site and degrading user experience, making it more vulnerable to attacks.

ACTION PLAN · STEPS TO FOLLOW

1. **Update all outdated plugins and themes** — URGENT

   This is the most urgent step. Outdated software is the main entry point for attackers. Make sure to update the two plugins that are currently behind.

2. **Enable Cloudflare CDN through SWPanel**

   This will act as a security shield, filtering out malicious traffic and bots before they reach your server. It's the easiest and most effective way to improve your site's protection.

3. **Harden WordPress login security**

   Change your WordPress login URL from wp-login.php to a custom one using a security plugin. This makes brute-force attacks much harder.

Analysis of SWPANEL.COM generated by SWPanel

Conclusions

4

Block access to sensitive files

Add the following rule to your .htaccess or Nginx config to prevent access to dangerous files like .env or wp-config.php.bak:

```
<FilesMatch "\.(env|bak|git|config|sql)$">
Order allow,deny
Deny from all
</FilesMatch>
```

5

Monitor and block suspicious IPs

Use Fail2Ban to automatically block IPs that show repeated malicious behavior, such as brute-force attempts or scanning.

I know this can feel overwhelming, but you're not alone in this. These are common issues that many websites face, and they can be resolved with the right steps. The most important thing is to act now—before a real breach happens. Start with updating your plugins and enabling Cloudflare, and I'll be here to help you with the rest.

Your site is still functional and not yet fully compromised, which gives us a window to fix things before it's too late. Just take the first step, and we'll go from there. You have the power to protect your site, and I'm here to make sure you do it right.

Analysis of SWPANEL.COM generated by SWPanel

Glossary of terms

A brief explanation of the technical terms used in this report.

Backdoor
hidden code that lets an attacker access and control the website remotely.

Brute force
massive attempts to guess a password by trying many combinations.

Cloaking
showing search engines different content from what visitors see; typical of SEO spam.

Database permissions (GRANT)
privileges that determine what a user can do in the database (INSERT, UPDATE...).

HTTP status codes (404, 5xx)
404 = page not found; 5xx = server error while processing the request.

Injection (SQL / URL)
inserting code or commands through a field or URL to run unintended actions.

Obfuscation
a technique to hide what the code really does (e.g. with base64_decode) and avoid detection.

Quantization
compressing the SWPanel AI Engine model so it uses less memory while keeping almost the same accuracy.

SEO spam
injected pages or links (betting, pharmacy...) to rank fraudulent content on your domain.

Timeout
the request takes too long and is aborted before completing.

Token
the smallest unit of text (a word or fragment) the SWPanel AI Engine processes; it measures the amount of computation.

Transient (WordPress)
temporary data that WordPress caches in the database.

Verdict (Clean / Suspicious / Compromised)
the security classification the analysis assigns to each file.

Analysis of SWPANEL.COM generated by SWPanel

Glossary of terms

Webshell
a malicious script that gives the attacker a console to run commands on the server.

Analysis of SWPANEL.COM generated by SWPanel

Technical statistics

Resources and compute invested to generate this report: log download and analysis and SWPanel AI Engine inference.

Execution time

8m 57s	6m 28s	2m 29s
TOTAL TIME	ANALYSIS TIME	PDF RENDERING

Logs analyzed

14	186.420	39,93 MB
LOGS DOWNLOADED	LINES ANALYZED	DATA PROCESSED

the provided logs
LAYERS REVIEWED

Errors and fixes

5	4	4
UNIQUE ERRORS	AFFECTED FILES	FIXES

2
CRITICAL ERRORS

SWPanel AI Engine compute

7	11.553	5.014
MODEL CALLS	INPUT TOKENS	GENERATED TOKENS

16.567	~42 tok/s
TOKENS PROCESSED	GENERATION SPEED

Analysis of SWPANEL.COM generated by SWPanel

Technical statistics

SWPanel AI Engine (analysis and writing)

qwen3-coder	qwen3moe	30.5B
SWPANEL AI ENGINE	FAMILY	PARAMETERS

Q8_0
QUANTIZATION

Compute infrastructure

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

80 GB HBM2e	2 TB/s	19,5 TFLOPS
VRAM	MEMORY BANDWIDTH	FP32

312 TFLOPS	221.184	80
FP16/BF16	CUDA THREADS	CPU THREADS

Energy consumed and its cost

0,062 kWh	0,093 kWh	0,155 kWh
IT DRAW (SERVER + GPU)	COOLING (X1.5)	TOTAL ENERGY

0,19 €
COMPUTE COST

Infrastructure cost (amortization)

0,61 €	0,155 kWh	38 g
HW AND NETWORK AMORTIZATION	INFRASTRUCTURE ENERGY	INFRASTRUCTURE CO2

Analysis of SWPANEL.COM generated by SWPanel

Technical statistics

0,83 €
ESTIMATED TOTAL COST

77 g
ESTIMATED CO2

HOW THESE FIGURES WERE COMPUTED

Metrics estimated on NVIDIA NVIDIA A100 infrastructure with the qwen3-coder:30b-a3b-q8_0 model. The server with the GPU draws ~575 W on average. Cooling adds 1.5 kW per kW of compute, so the total draw is ~2.5 times the compute (PUE 2.5). Energy is computed over the real analysis time at 0.185 EUR/kWh, compute cost at a reference cloud rate (~1.8 EUR/h) and CO2 at 250 g/kWh. Approximate values to size the effort behind this report.

EFFICIENT TECHNOLOGY

This analysis runs on our own infrastructure with the SWPanel AI Engine (local models), without sending your code to third parties. Detecting and fixing errors early avoids rework, downtime and unnecessary server resource usage.

A SMALL ACT OF LOVE FOR THE PLANET

Creating this report left a footprint of about 77 g of CO2. Behind every analysis there is energy, water and resources from the only home we all share. We ask you for a small act of love: request only the reports you truly need and avoid printing them, to protect the forests, the air and the lives of those who come after us. Caring for the Earth is caring for one another. Thank you, from the heart, for leaving a lighter footprint and a greener tomorrow.

Analysis of SWPANEL.COM generated by SWPanel

swpanel

https://www.swpanel.com

Document: SW-COD-EJEMPLO-2026

Date: 16/10/2026