# Wordpress Scanner with WPScan Report

**https://dgtalbug.dev/**

Blogging Website developed and maintained by https://dgtalbug.dev/

The Light Wordpress Scanner didn't check for outdated plugins, config files, database exports, and more. Upgrade now to run comprehensive Deep scans.

## Summary

**Overall risk level:**

Low

**Risk ratings:**

| | |
|---|---|
| Critical: | 0 |
| High: | 0 |
| Medium: | 0 |
| Low: | 1 |
| Info: | 6 |

**Scan information:**

| | |
|---|---|
| Start time: | Nov 01, 2025 / 22:52:53 UTC+0530 |
| Finish time: | Nov 01, 2025 / 22:54:00 UTC+0530 |
| Scan duration: | 1 min, 7 sec |
| Tests performed: | 7/7 |
| Scan status: | Finished |

## Findings

### Found wp-cron file

| URL | Found by |
|---|---|
| https://dgtalbug.dev/wp-cron.php | Direct Access (Aggressive Detection) |

Details

**Risk description:**
The wp-cron.php file is responsible for scheduled events in a WordPress website. By default, when a request is made, WordPress will generate an additional request from it to the wp-cron.php file. By generating a large number of requests to the website, it is therefore possible to make the site perform a DoS attack on itself.

**Recommendation:**
Add the variable DISABLE_WP_CRON to true in the file wp-config.php and restrict access to the file wp-cron.php.

**References:**
https://www.iplocation.net/defend-wordpress-from-ddos

**Classification:**
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

### Interesting headers found

| URL | Found by | Interesting Entries |
|---|---|---|
| https://dgtalbug.dev/ | Headers (Passive Detection) | server: LiteSpeed<br>x-turbo-charged-by: LiteSpeed |

Details

**Risk description:**
The HTTP headers returned by the server often contain information about the specific software type and version that is running. This information could be used by an attacker to mount specific attacks against the server and the application.

**Recommendation:**
It is recommended that a tester inspects this issue manually to find out if it can be escalated to higher-risk vulnerabilities.

**Classification:**
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

## Found robots.txt file

| URL | Found by | Interesting Entries |
|---|---|---|
| https://dgtalbug.dev/robots.txt | Robots Txt (Aggressive Detection) | /wp-admin/<br>/wp-admin/admin-ajax.php |

Details

**Risk description:**
The robots.txt file sometimes contains URLs that should be hidden from public view. However, this should not be considered a security measure since anyone can read the robots.txt file and discover those hidden paths.

**Recommendation:**
Review the contents of the robots.txt file and remove the URLs which point to sensitive locations in the application. These locations should be protected by strong access control mechanisms and require proper authorization.

**References:**
https://www.theregister.co.uk/2015/05/19/robotstxt/

**Classification:**
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

## Main WordPress Theme Revision detected

| Theme information |
|---|
| Theme name: revision |
| Theme version: 1.0.7 |
| Location: https://dgtalbug.dev/wp-content/themes/revision/ |
| Style URL: https://dgtalbug.dev/wp-content/themes/revision/style.css?ver=1.0.7 |
| Style name: Revision |
| Style uri: https://revision.codesupply.co |
| Description: High-Performance WordPress Personal Blog Theme |
| Author: Code Supply Co. |
| Author uri: https://codesupply.co |
| License: GNU General Public License version 3.0 |
| License uri: http://www.gnu.org/licenses/gpl-3.0.html |
| Tags: custom-colors, editor-style, theme-options, custom-menu, sticky-post, right-sidebar, translation-ready |
| Text domain: revision |
| Found by: Css Style In Homepage (Passive Detection) |

## Scan finished successfully

## WordPress 6.8.3 has no known vulnerabilities

Main theme Revision has no known vulnerabilities

## Scan coverage information

### List of tests performed (7/7)

- Scanning with WPScan (this may take a while)...
- Checking for valuable information in HTTP headers...
- Checking for the robots.txt file...
- Checking whether wp-cron is enabled...
- Searching for WordPress vulnerabilities...
- Searching for main theme vulnerabilities...
- Searching information for main theme: revision

### Scan parameters

| | |
|---|---|
| Target: | https://dgtalbug.dev/ |
| Detection mode: | Passive |
| Enumerate users: | False |
| Enumerate vulnerable plugins: | False |
| Enumerate vulnerable themes: | False |
| Enumerate config backups: | False |
| Enumerate database exports: | False |
| Enumerate TimThumbs: | False |
| Scan Type: | Light |
| Authentication: | False |