Wordpress Scanner with WPScan Report (Light)

https://www.gabrieleviola.it/
Target added due to a redirect from https://gabrieleviola.it

The Light Wordpress Scanner didn't check for outdated plugins, config files, database exports, and more.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:	3
Info:	4

Scan information:

Start time:	Apr 06, 2025 / 18:30:46 UTC+03
Finish time:	Apr 06, 2025 / 18:31:07 UTC+03
Scan duration:	21 sec
Tests performed:	7/7
Scan status:	Finished

Findings

Interesting headers found

URL	Found by	Interesting Entries
https://www.gabrieleviola.it/	Headers (Passive Detection)	server: aruba-proxy x-servername: webx.aruba.it x-aruba-cache: HIT alt-svc: h3=":443"; ma=86400

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://www.gabrieleviola.it/robots.txt	Robots Txt (Aggressive Detection)	/wp-admin/ /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

Found wp-cron file

URL	Found by
https://www.gabrieleviola.it/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

Main WordPress Theme gabrieleviola detected

Theme information
Theme name: gabrieleviola Theme version: 1.0 Location: https://www.gabrieleviola.it/wp-content/themes/gabrieleviola/ Style URL: https://www.gabrieleviola.it/wp-content/themes/gabrieleviola/style.css Style name: gabrieleviola Style uri: gabrieleviola.it Description: sito web v.7.7.3 Author: Gabriele Viola Author uri: gabrieleviola.it License: GNU General Public License v2 or later License uri: http://www.gnu.org/licenses/gpl-2.0.html Tags: sito web Text domain: gabrieleviola Found by: Urls In 404 Page (Passive Detection)

Scan finished successfully

WordPress version was not detected

Main theme gabrieleviola 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: gabrieleviola

Scan parameters

Target:	https://www.gabrieleviola.it/
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