

Website Recon Report

✓ <https://dgtalbug.dev/>

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

Summary

Overall risk level:

Low

Risk ratings:

Critical: 0

High: 0

Medium: 0

Low: 1

Info: 1

Scan information:

Start time: Nov 01, 2025 / 22:52:11 UTC+0530

Finish time: Nov 01, 2025 / 22:58:03 UTC+0530

Scan duration: 5 min, 52 sec

Tests performed: 2/2




















Scan status: **Finished**

Findings

Server software and technology found

port 443/tcp

UNCONFIRMED ⓘ

Software / Version	Category
 Clipboard.js	JavaScript libraries
 Contact Form 7 6.1.3	WordPress plugins, Form builders
 Font Awesome	Font scripts
 jQuery Migrate 3.4.1	JavaScript libraries
 wordpress-contact-form-7	Miscellaneous
 wordpress-loginizer	Miscellaneous
 wordpress-regenerate-thumbnails	Miscellaneous
 contact-form-7	Miscellaneous
 Google Font API	Font scripts
 Gravatar	Miscellaneous
 jQuery 3.7.1	JavaScript libraries
 LiteSpeed	Web servers
 Lightbox	JavaScript libraries
 MySQL	Databases
 PHP	Programming languages
 Sectigo	SSL/TLS certificate authorities
 Smash Balloon Instagram Feed	WordPress plugins
 Swiper	JavaScript libraries
 WordPress 6.8.3	CMS, Blogs

 Custom Twitter Feeds	Widgets, WordPress plugins
 Instagram Feed for WordPress	Widgets, WordPress plugins
 Google AdSense	Advertising
 Google Tag Manager	Tag managers
 jsDelivr	CDN
 Lodash 1.13.7	JavaScript libraries
 HSTS	Security
 RSS	Miscellaneous

▼ Details

Risk description:

The risk is that an attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:

We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

References:

https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html

Classification:

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

Screenshot:

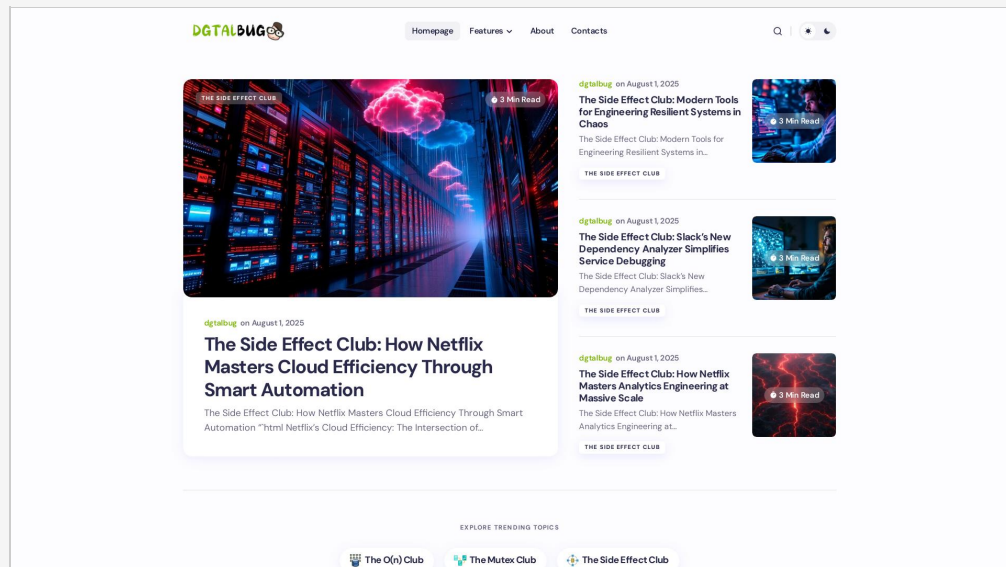


Figure 1. Website Screenshot

 Website is accessible.

Scan coverage information

List of tests performed (2/2)

- ✓ Test initial connection
- ✓ Scanned for website technologies

Scan parameters

Target: https://dgtalbug.dev/

Scan stats

Total number of HTTP requests:	3
Average time until a response was received:	2990ms
