WordPress Security Analysis

https:// www.test-url.com

This report presents the results of a passive analysis of HTTP responses for the target WordPress site.

WORDPRESS VERSION

6.5.7

Version not latest release (6.9)

Update Now (see releases)

4

ISSUES FOUND

- Username enumeration
- Core version not latest release
- Plugin needs updating
- PHP End of Life

Page Title: www.test-url.com

Certificate:

- valid to: 2026-02-26

TLS 1.2

IP Address:

123.456.789.123

Hosting Provider:

AXARNET-AS, ES (AS50926)

Web Server:

Apache

X-Powered-By:

PHP/7.4.33, PleskLin

PHP Version:

7.4.33

WARNING **- PHP End of Life (no support)**

Shared Hosting:

175 sites found on IP

Blocklists & Threat Intel

Blocklist and threat intelligence sources were searched for references to the target IP address and hostname.

Dshield (host blocklist)	Clean	**abuse.ch** (feodo list)	Clean
Alienvault OTX (blacklist)	Clean	**URLhaus**	Clean
Cisco Talos (blacklist)	Clean	**Spamhaus** (drop / edrop)	Clean

The nature of threat intelligence and block lists can result in **false negatives** and **false positives** are possible. If using shared hosting; a blocklisting may be due to a compromised site on any tenant on the host (as IP address is shared).

Referenced resources are used by security professionals. These resources may contain links to live malware.

WordPress Plugins

The following plugins were detected through analysis of the HTML source from the sites main page.

PLUGIN	UPDATE STATUS	ABOUT
dflip	Unknown	
woocommerce (9.1.1)	Not Current	latest release (**10.4.3**) https://woocommerce.com/
divi-builder	Unknown	
wp-pagenavi	Unknown	latest release (**2.94.5**) https://lesterchan.net/portfolio/programming/php/
divi_extended_column_layouts	Unknown	
elementor	Unknown	latest release (**3.34.2**) https://elementor.com/
mailchimp-for-woocommerce	Unknown	latest release (**5.6**) https://mailchimp.com/connect-your-store/
divi-bodycommerce	Unknown	

Plugins are a common source of security vulnerabilities within WordPress installations. Always keep them updated to the latest version and monitor the developers page for security related updates and fixes.

There are likely more plugins installed than those listed here as the detection method used here is passive. While these results give an indication of the status of plugin updates, a more comprehensive assessment can be performed by brute forcing the plugin paths using a **specialist tool**.

WordPress Themes

Themes have been detected by examining paths under `/wp-content/themes/`. The active theme is highlighted.

	THEME DETAILS	URL
	Divi 4.26.0	http://www.elegantthemes.com/gallery/divi/

The code that makes up a theme can contain security vulnerabilities. Always keep themes updated to the latest version and monitor the developers page for security related updates and fixes.

> The **active theme** is highlighted and found in the HTML source of the page. A comprehensive assessment should include checking for other themes that are installed but not active as these can also contain exploitable security vulnerabilities. Remove all unused themes to **minimise the attack surface** of the WordPress installation.

User Enumeration

The first two user ID's were tested to determine if user enumeration is possible.

	USERNAME	ACCOUNT NAME
ID: 1	error getting page	
ID: 2	error getting page	

It is recommended to rename the `admin` user account to reduce the chance of brute force attacks occurring. Strong passwords on all accounts are of course essential; renaming the **admin account** simply adds an extra layer of protection especially useful against automated attackers (bots).

Keep in mind that if the author archives are enabled it is usually **possible to enumerate all users** within a WordPress installation. Including a renamed `admin` account.

> Password attacks are common; reduce their effectiveness with rate limiting, CAPTCHAs and MFA on login forms.

WordPress API Endpoints

This test checks if key WordPress API endpoints are accessible from the public internet. Public access to these APIs may expose sensitive information such as usernames, post content, or configuration details. The `xmlrpc.php` endpoint, in particular, has historically been a target for brute-force and pingback amplification attacks.

	ENDPOINT	STATUS	HTTP CODE
	/wp-json/wp/v2/pages	✔ Restricted	None
	/wp-json/wp/v2/posts	✔ Restricted	None
	/wp-json/wp/v2/users	✔ Restricted	None
	/xmlrpc.php	✔ Restricted	None

If your site does not require these APIs to be publicly accessible, consider restricting access using web server rules or authentication to reduce the attack surface. You can also disable unused APIs via plugins or filters.

Exposed Backup/Config Files

This check looks for common backup or misplaced configuration files that, if exposed, can leak database credentials or other sensitive information.

	PATH	HTTP	SIZE	URL
✔	No exposed backup/config files detected			

Immediately remove publicly accessible backups and ensure sensitive files are never placed within the web root. Consider using deny rules to block access to known sensitive paths.

Directory Indexing

In the test we attempted to list the directory contents of the uploads and plugins folders to determine if **Directory Indexing** is enabled. This vulnerability type is known as information leakage and can reveal sensitive information regarding your site configuration or content.

	PATH	STATUS
	/wp-content/uploads/	✔ Restricted
	/wp-content/plugins/	✔ Restricted

Directory indexing was tested on the `/wp-content/uploads/` and `/wp-content/plugins/` directores. Note that other directories may have this web server feature enabled, so ensure you check other folders in your installation. It is good practice to ensure directory indexing is disabled for your full WordPress installation either through the web server configuration or `.htaccess`.

Linked Sites

Details for each linked external host have been gathered. Includes blocklist check, ASN lookup for hosting provider and geoip lookup. Links with poor reputation could indicate a compromise or may be a threat to users of the site.

	LINKED / HOST	IP	COMPANY / HOST	COUNTRY
✔	api.whatsapp.com	57.144.197.32 (AS32934)	FACEBOOK, US	??
✔	www.google.com	192.178.219.99 (AS15169)	GOOGLE, US	??
✔	es-es.facebook.com	57.144.22.141 (AS32934)	FACEBOOK, US	??
✔	www.instagram.com	57.144.22.34 (AS32934)	FACEBOOK, US	??
✔			AXARNET-AS, ES	??

IP address is checked against multiple threat intelligence providers and blocklists.

Linked Javascript

Compromised sites will often be linked to malicious `javascript` or `iframes` in an attempt to attack users of your site. Audit the listed scripts and investigate any suspicious entries. Remove unused JavaScript and other resources to improve load times and reduce the attack surface.

	LINKED JAVASCRIPT	COMPANY / HOST	COUNTRY
✔	https://www.google.com/recaptcha/api.js?render=6Ld_xE8cAAAAAO-0uzgwI0T...	GOOGLE, US	??
✔	https:// www.test-url.com /wp-includes/js/comment-reply.min.js?ver=6.5.7	AXARNET-AS, ES	??
✔	https:// www.test-url.com /wp-includes/js/jquery/jquery-migrate.min.js?ver=3.4.1	AXARNET-AS, ES	??
✔	https:// www.test-url.com /wp-content/plugins/woocommerce/assets/js/fron...	AXARNET-AS, ES	??
✔	https:// www.test-url.com /wp-content/plugins/woocommerce/assets/js/js-c...	AXARNET-AS, ES	??
✔	https:// www.test-url.com /wp-content/themes/Divi/js/smoothscroll.js?ver=4.26.0	AXARNET-AS, ES	??
✔	https:// www.test-url.com /wp-content/themes/Divi/core/admin/js/recaptcha.js?ver=4.26.0	AXARNET-AS, ES	??
✔	https:// www.test-url.com /wp-content/themes/Divi/includes/builder/featu...	AXARNET-AS, ES	??
✔	https:// www.test-url.com /wp-content/plugins/woocommerce/assets/js/sour...	AXARNET-AS, ES	??
✔	https:// www.test-url.com /wp-content/plugins/divi-bodycommerce/scripts/...	AXARNET-AS, ES	??
✔	https://www.googletagmanager.com/gtag/js?id=G-T3LNHX0WMV	GOOGLE, US	??
✔	https:// www.test-url.com /wp-content/plugins/dflip/assets/js/dflip.min.js?ver=1.7.5.1	AXARNET-AS, ES	??
✔	https:// www.test-url.com /wp-content/plugins/woocommerce/assets/js/fron...	AXARNET-AS, ES	??
✔	https:// www.test-url.com /wp-content/themes/Divi/includes/builder/featu...	AXARNET-AS, ES	??
✔	https:// www.test-url.com /wp-content/plugins/woocommerce/assets/js/fron...	AXARNET-AS, ES	??
✔	https:// www.test-url.com /wp-content/plugins/woocommerce/assets/js/jque...	AXARNET-AS, ES	??
✔	https:// www.test-url.com /wp-content/plugins/mailchimp-for-woocommerce/...	AXARNET-AS, ES	??
✔	https:// www.test-url.com /wp-content/themes/Divi/js/scripts.min.js?ver=4.26.0	AXARNET-AS, ES	??
✔	https:// www.test-url.com /wp-content/themes/Divi/includes/builder/featu...	AXARNET-AS, ES	??
✔	https://www.googletagmanager.com/gtag/js?id=G-T3LNHX0WMV	GOOGLE, US	??

	LINKED JAVASCRIPT	COMPANY / HOST	COUNTRY
✔	https:// www.test-url.com /wp-content/themes/Divi/includes/builder/featu...	AXARNET-AS, ES	??
✔	https:// www.test-url.com /wp-content/themes/Divi/core/admin/js/common.js?ver=4.26.0	AXARNET-AS, ES	??
✔	https:// www.test-url.com /wp-includes/js/jquery/jquery.min.js?ver=3.7.1	AXARNET-AS, ES	??
✔	https:// www.test-url.com /wp-content/plugins/divi-bodycommerce/scripts/...	AXARNET-AS, ES	??
✔	https:// www.test-url.com /wp-content/themes/Divi/includes/builder/featu...	AXARNET-AS, ES	??
✔	https://cdn-cookieyes.com/client_data/6280663e6ebad7760dfd9386/script.js	CLOUDFLARENET, US	??
✔	https:// www.test-url.com /wp-content/themes/Divi/includes/builder/featu...	AXARNET-AS, ES	??
✔	https:// www.test-url.com /wp-content/themes/Divi/includes/builder/featu...	AXARNET-AS, ES	??
✔	https:// www.test-url.com /wp-content/themes/Divi/core/admin/js/es6-prom...	AXARNET-AS, ES	??

IP address is checked against multiple threat intelligence providers and blocklists.