WordPress Security Analysis (Passive)

https://www.bbaa.uma.es/blog/

Results of a passive (non-intrusive) security analysis of the target WordPress site.

Core Version

5.2.9

Version not latest release (5.5.3)

Update Now (see releases)

SERVER DETAILS

Web Server:
Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.3.7

X-Powered-By:
PHP/7.3.7

PHP Version:
7.3.7

IP Address:
150.214.45.146 (150.214.0.0/16)

Hosting Provider:
CICA Centro Informatico Cientifico de Andalucia - CICA, ES (AS198096)

Shared Hosting:
93 sites found on IP

3 issues

Issues found during a high level analysis of the target.

Blacklists & Threat Intel

Blacklist 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 blacklisting means **false negatives** and **false positives** are both possible. If the site is utilizing shared hosting; a blacklisting may be due to a compromised site on any tenant on the host (as the IP address is shared).

⚠ Referenced resources are used by security professionals around the world. Due to the nature of the work the sites 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
	fourteen-colors (1.6)	CURRENT	latest release (**1.6**) http://celloexpressions.com/plugins/fourteen-colors
	flickr-badges-widget (1.2.7)	UNKNOWN	
	pdf-embedder (4.4)	UPDATE	latest release (**4.6.1**) http://wp-pdf.com/

Plugins are a source of many security vulnerabilities within WordPress installations, always keep them updated to the latest version available and check the developers plugin page for information about 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 Theme

The theme has been found by examining the path `/wp-content/themes/ *theme name* /`

	THEME DETAILS	URL
	Twenty Fourteen 2.7	https://wordpress.org/themes/twentyfourteen/

While plugins get a lot of attention when it comes to security vulnerabilities, themes are another source of security vulnerabilities within WordPress installations. Always keep themes updated to the latest version available and check the developers theme page for information about updates and fixes.

> The theme listed here is the **active theme** found in the HTML source of the page. Installed but not active themes may contain security vulnerabilities. Remove any 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	not found	
ID: 2	not found	

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.

> Only the first two user ID's were tested during this scan. Try the **advanced membership options** or a dedicated tool for a thorough enumeration of users, themes and plugins.

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/	**Indexing Enabled**
	/wp-content/plugins/	**indexing disabled**

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 blacklist 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
✔	www.latermicamalaga.com	82.159.164.148 (AS6739)	ONO-AS Cableuropa - ONO, ES	ES
✔	slash-paris.com	163.172.140.109 (AS12876)	Online SAS, FR	FR
✔	w3art.es	unable to resolve (AS)		??
✔	salonkritik.net	207.148.19.116 (AS20473)	AS-CHOOPA	US
✔	es.wordpress.org	198.143.164.252 (AS32475)	SINGLEHOP-LLC	US

☞ First column check gives an indication of host IP address cross referenced against multiple threat intelligence providers and blacklists.

Linked Javascript

Compromised sites will often be linked to malicious `javascript` or `iframes` in an attempt to attack users of your site. Look over the listed scripts and investigate ones you are not sure. Legitimate scripts should be also examined as removal of unused javascript code may speed up the site and reduce the attack surface.

	LINKED JAVASCRIPT	COMPANY / HOST	COUNTRY
✔	https://www.bbaa.uma.es/blog/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp	CICA Centro Informatico Cientifico de Andalucia - CICA, ES	ES
✔	https://www.bbaa.uma.es/blog/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1	CICA Centro Informatico Cientifico de Andalucia - CICA, ES	ES
✔	https://www.bbaa.uma.es/blog/wp-content/themes/twentyfourteen/js/functions.js?ver=20150315	CICA Centro Informatico Cientifico de Andalucia - CICA, ES	ES
✔	https://www.bbaa.uma.es/blog/wp-includes/js/jquery/jquery.masonry.min.js?ver=3.1.2b	CICA Centro Informatico Cientifico de Andalucia - CICA, ES	ES
✔	https://www.bbaa.uma.es/blog/wp-includes/js/imagesloaded.min.js?ver=3.2.0	CICA Centro Informatico Cientifico de Andalucia - CICA, ES	ES
✔	https://www.bbaa.uma.es/blog/wp-includes/js/masonry.min.js?ver=3.3.2	CICA Centro Informatico Cientifico de Andalucia - CICA, ES	ES
✔	https://www.flickr.com/badge_code_v2.gne?count=9&display=random&size=s&layout=x&source=user&user=103100525@N06	AMAZON-02	US
✔	https://www.bbaa.uma.es/blog/wp-includes/js/wp-embed.min.js?ver=5.2.9	CICA Centro Informatico Cientifico de Andalucia - CICA, ES	ES

First column check gives an indication of host IP address cross referenced against multiple threat intelligence providers and blacklists. Keep in mind that legitimate scripts may have malicious code appended to them following a compromise.