Pentest-Tools.com

WordPress Vulnerability Scanner - WPScan Report

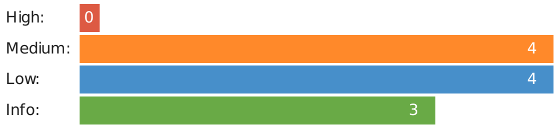
✓ http://demo.pentest-tools.com/wordpress/

Summary

Overall risk level:

Medium

Risk ratings:



Scan information:

Start time:	2018-06-28 14:09:04
Finish time:	2018-06-28 14:09:16
Scan duration:	12 sec
Tests performed:	11/11
Scan status:	Finished

Findings

Upload directory has listing enabled

URL: http://demo.pentest-tools.com/wordpress/wp-content/uploads/

Found by: Direct Access (Aggressive Detection)

Details

Risk description:
Directory listing can expose sensitive files from the affected location - which may contain confidential information.

Recommendation:
Reconfigure the web server to deny directory listing.

WordPress 4.8.3 has 10 vulnerabilities

	Vulnerability title	Fixed in	CVE	CVSS	Reference URLs
●	WordPress 3.7-4.9 - 'newbloguser' Key Weak Hashing	4.8.4	2017-17091	6.5	https://wordpress.org/news/2017/11/wordpress-4-9-1-security-and-maintenance-release/ https://github.com/WordPress/WordPress/commit/eaf1cfdc1fe0bdffabd8d879c591b864d833326c
●	WordPress 3.7-4.9.4 - Remove localhost Default	4.8.6	2018-10101	5.8	https://wordpress.org/news/2018/04/wordpress-4-9-5-security-and-maintenance-release/ https://github.com/WordPress/WordPress/commit/804363859602d4050d9a38a21f5a65d9aec18216
●	WordPress 3.7-4.9.4 - Use Safe Redirect for Login	4.8.6	2018-10100	5.8	https://wordpress.org/news/2018/04/wordpress-4-9-5-security-and-maintenance-release/ https://github.com/WordPress/WordPress/commit/14bc2c0a6fde0da04b47130707e01df850eedc7e
●	WordPress <= 4.9.4 - Application Denial of Service (DoS) (unpatched)	N/A	2018-6389	5	https://baraktawily.blogspot.fr/2018/02/how-to-dos-29-of-world-wide-websites.html https://github.com/quitten/doser.py https://thehackernews.com/2018/02/wordpress-dos-exploit.html
●	WordPress 2.3-4.8.3 - Host Header Injection in Password Reset	N/A	2017-8295	4.3	https://exploitbox.io/vuln/WordPress-Exploit-4-7-Unauth-Password-Reset-0day-CVE-2017-8295.html http://blog.dewhurstsecurity.com/2017/05/04/exploitbox-wordpress-security-advisories.html https://core.trac.wordpress.org/ticket/25239
					https://github.com/WordPress/WordPress/commit/3fe9cb61ee71fcfadb5e002399296fcc1198d850

●	WordPress 3.7-4.9.1 - MediaElement Cross-Site Scripting (XSS)	4.8.5	2018-5776	4.3	https://wordpress.org/news/2018/01/wordpress-4-9-2-security-and-maintenance-release/ https://core.trac.wordpress.org/ticket/42720
●	WordPress 3.7-4.9.4 - Escape Version in Generator Tag	4.8.6	2018-10102	4.3	https://wordpress.org/news/2018/04/wordpress-4-9-5-security-and-maintenance-release/ https://github.com/WordPress/WordPress/commit/31a4369366d6b8ce30045d4c838de2412c77850d
●	WordPress 2.8.6-4.9 - Authenticated JavaScript File Upload	4.8.4	2017-17092	3.5	https://wordpress.org/news/2017/11/wordpress-4-9-1-security-and-maintenance-release/ https://github.com/WordPress/WordPress/commit/67d03a98c2cae5f41843c897f206adde299b0509
●	WordPress 1.5.0-4.9 - RSS and Atom Feed Escaping	4.8.4	2017-17094	3.5	https://wordpress.org/news/2017/11/wordpress-4-9-1-security-and-maintenance-release/ https://github.com/WordPress/WordPress/commit/f1de7e42df29395c3314bf85bff3d1f4f90541de
●	WordPress 4.3.0-4.9 - HTML Language Attribute Escaping	4.8.4	2017-17093	3.5	https://wordpress.org/news/2017/11/wordpress-4-9-1-security-and-maintenance-release/ https://github.com/WordPress/WordPress/commit/3713ac5ebc90fb2011e98dfd691420f43da6c09a

Details

Risk description:
Depending on the specific details of the vulnerabilities, an attacker could exploit them to affect the confidentialy and the integrity of the application's data or to affect the availability of the entire system.

Recommendation:
Update the WordPress to the latest version.

Plugin newsletters-lite 4.6.4.2 has 1 vulnerabilities

last_updated: 2018-03-12T13:42:00.000Z

plugin_version: 4.6.4.2

latest_version: 4.6.8.6

plugin_name: newsletters-lite

found_by: Urls In Homepage (Passive Detection)

outdated: True

location: http://demo.pentest-tools.com/wordpress/wp-content/plugins/newsletters-lite/

	Vulnerability title	Fixed in	CVE	CVSS	Reference URLs
●	Tribulant Newsletters <= 4.6.4.2 â€“ Multiple Vulnerabilities	4.6.5	N/A	N/A	http://defensecode.com/advisories/DC-2017-01-012_WordPress_Tribulant_Newsletters_Plugin_Advisory.pdf

Details

Risk description:
Vulnerable WordPress plugins are a common way to compromise a WordPress application. Depending on the specific details of the plugin vulnerabilities, an attacker could exploit them in order to affect the confidentialy and the integrity of the application's data or to affect the availability of the entire system.

Recommendation:
Update the affected plugin to the latest version.

Found 1 users

admin

Details

Risk description:
An attacker could try to brute-force the passwords of these users and gain unauthorized access to their WordPress accounts. As a result, the attacker could modify the content of the website, add scandalous/malicious pages or just delete the existing content.

Recommendation:
Make sure that the WordPress users have strong passwords.

Reconfigure WordPress to deny user enumeration.
More details can be found here:
https://perishablepress.com/stop-user-enumeration-wordpress/

Interesting headers found

URL: http://demo.pentest-tools.com/wordpress/

Found by: Headers (Passive Detection)

Interesting entries:

- Server: Apache/2.4.10 (Debian)

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:
Reconfigure the web server in order to hide specific information about software type and version in the HTTP headers.

Found robots.txt file

URL: http://demo.pentest-tools.com/wordpress/robots.txt

Found by: Robots Txt (Aggressive Detection)

Details

Risk description:
The robots.txt file sometimes contains URLs which 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.

Found xmlrpc file

URL: http://demo.pentest-tools.com/wordpress/xmlrpc.php

Found by: Direct Access (Aggressive Detection)

Details

Risk description:
The xmlrpc.php file is a standard component of WordPress, however, it could be used to implement attacks against other websites such as brute-force amplification attacks.

For more info, check the following resources:
http://codex.wordpress.org/XML-RPC_Pingback_API

Recommendation:
Block access to the xmlrpc.php file using a protection mechanism such as the .htaccess file or a Web Application Firewall.

Found default Readme file

URL: http://demo.pentest-tools.com/wordpress/readme.html

Found by: Direct Access (Aggressive Detection)

Details

Risk description:
The Readme file contains information which could help an attacker to fingerprint the exact version of WordPress that is running, which might be helpful for mounting further attacks.

Recommendation:
Remove the Readme file.

Main theme twentyseventeen 1.2 has no known vulnerabilities.

last_updated: 2018-04-03T00:00:00.000Z

theme_name: twentyseventeen

license: GNU General Public License v2 or later author: the WordPress team

style_url: http://demo.pentest-tools.com/wordpress/wp-content/themes/twentyseventeen/style.css?ver=4.8.3

description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a focus on business sites, it features multiple sections on the front page as well as widgets, navigation and social menus, a logo, and more. Personalize its asymmetrical grid with a custom color scheme and showcase your multimedia content with post formats. Our default theme for 2017 works great in many languages, for any abilities, and on any device.

tags: one-column, two-columns, right-sidebar, flexible-header, accessibility-ready, custom-colors, custom-header, custom-menu, custom-logo, editor-style, featured-images, footer-widgets, post-formats, rtl-language-support, sticky-post, theme-options, threaded-comments, translation-ready

latest_version: 1.5

author_uri: https://wordpress.org/

license_uri: http://www.gnu.org/licenses/gpl-2.0.html

style_name: Twenty Seventeen

text_domain: twentyseventeen

found_by: Css Style (Passive Detection)

style_uri: https://wordpress.org/themes/twentyseventeen/

theme_version: 1.2

outdated: True

location: http://demo.pentest-tools.com/wordpress/wp-content/themes/twentyseventeen/

Details

Risk description:
The current WordPress theme does not have any known vulnerabilities.

Recommendation:
No recommendations for this issue

No additional themes found

Scan finished successfully

Scan coverage information

List of tests performed (11/11)

- ✓ Scanning with WPScan...
- ✓ Checking for interesting findings: http://demo.pentest-tools.com/wordpress/
- ✓ Checking for interesting findings: http://demo.pentest-tools.com/wordpress/robots.txt
- ✓ Checking for interesting findings: http://demo.pentest-tools.com/wordpress/xmlrpc.php
- ✓ Checking for interesting findings: http://demo.pentest-tools.com/wordpress/readme.html
- ✓ Checking for interesting findings: Upload directory has listing enabled
- ✓ Searching for WordPress vulnerabilities...
- ✓ Searching for main theme vulnerabilities...
- ✓ Searching for additional themes...
- ✓ Searching vulnerabilities for plugin newsletters-lite
- ✓ Attempting user enumeration...

Scan parameters

Target:	http://demo.pentest-tools.com/wordpress/