Pentest Tools

WordPress Vulnerability Scanner - WPScan Report

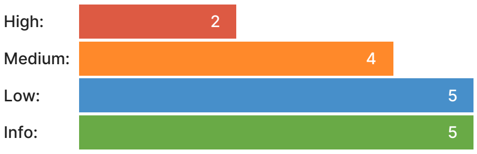
✓ http://testing1.pentest-tools.com:9000

Summary

Overall risk level:

High

Risk ratings:



Scan information:

Start time:	2023-03-21 15:16:53 UTC+02
Finish time:	2023-03-21 15:20:09 UTC+02
Scan duration:	3 min, 16 sec
Tests performed:	16/16
Scan status:	Finished

Findings

Vulnerabilities found for WordPress version

Risk level	Vulnerability title	Fixed in	CVE	CVSS	Reference URLs
●	WordPress <= 5.2.3 - Server-Side Request Forgery (SSRF) in URL Validation	5.1.3	2019-17669	9.8	https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/ https://github.com/WordPress/WordPress/commit/9db44754b9e4044690a6c32fd74b9d5fe26b07b2 https://blog.wpscan.com/wordpress/security/release/2019/10/15/wordpress-524-security-release-breakdown.html
●	WordPress <= 5.3 - wp_kses_bad_protocol() Colon Bypass	5.1.4	2019-20041	9.8	https://wordpress.org/news/2019/12/wordpress-5-3-1-security-and-maintenance-release/ https://github.com/WordPress/wordpress-develop/commit/b1975463dd995da19bb40d3fa0786498717e3c53
●	WordPress <= 5.2.3 - Admin Referrer Validation	5.1.3	2019-17675	8.8	https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/ https://github.com/WordPress/WordPress/commit/b183fd1cca0b44a92f0264823dd9f22d2fd8b8d0 https://blog.wpscan.com/wordpress/security/release/2019/10/15/wordpress-524-security-release-breakdown.html
●	WordPress < 5.8.3 - SQL Injection via WP_Query	5.1.12	2022-21661	8.6	https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-6676-cqfm-gw84 https://hackerone.com/reports/1378209
●	WordPress < 5.8 - Plugin Confusion	5.8	2021-44223	8.2	https://vavkamil.cz/2021/11/25/wordpress-plugin-confusion-update-can-get-you-pwned/
●	WordPress <= 5.2.3 - JSON Request Cache Poisoning	5.1.3	2019-17673	7.5	https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/ https://github.com/WordPress/WordPress/commit/b224c251adfa16a5f84074a3c0886270c9df38de https://blog.wpscan.com/wordpress/security/release/2019/10/15/wordpress-524-security-release-breakdown.html
●	WordPress 4.1-5.8.2 - SQL Injection via WP_Meta_Query	5.1.12	2022-21664	6.8	https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-jp3p-gw8h-6x86

●	WordPress 3.7 to 5.7.1 - Object Injection in PHPMailer	5.1.10	2020-36326	6.6	https://github.com/WordPress/WordPress/commit/267061c9595fedd321582d14c21ec9e7da2dcf62 https://wordpress.org/news/2021/05/wordpress-5-7-2-security-release/ https://github.com/PHPMailer/PHPMailer/commit/e2e07a355ee8ff36aba21d0242c5950c56e4c6f9 https://www.wordfence.com/blog/2021/05/wordpress-5-7-2-security-release-what-you-need-to-know/
●	WordPress < 5.4.2 - Misuse of set-screen-option Leading to Privilege Escalation	5.1.6	2020-4050	6.5	https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/ https://github.com/WordPress/WordPress/commit/dda0ccdd18f6532481406cabede19ae2ed1f575d https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-4vpv-fgg2-gcqc
●	WordPress < 5.4.2 - Authenticated XSS via Media Files	5.1.6	2020-4047	6.3	https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/ https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-8q2w-5m27-wm27
●	WordPress <= 5.2.2 - Cross-Site Scripting (XSS) in URL Sanitisation	5.1.2	2019-16222	6.1	https://wordpress.org/news/2019/09/wordpress-5-2-3-security-and-maintenance-release/ https://github.com/WordPress/WordPress/commit/30ac67579559fe42251b5a9f887211bf61a8ed68 https://hackerone.com/reports/339483
●	WordPress 5.0-5.2.2 - Authenticated Stored XSS in Shortcode Previews	5.1.2	2019-16219	6.1	https://wordpress.org/news/2019/09/wordpress-5-2-3-security-and-maintenance-release/ https://fortiguard.com/zeroday/FG-VD-18-165 https://www.fortinet.com/blog/threat-research/wordpress-core-stored-xss-vulnerability.html
●	WordPress <= 5.2.3 - Stored XSS in Style Tags	5.1.3	2019-17672	6.1	https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/ https://blog.wpscan.com/wordpress/security/release/2019/10/15/wordpress-524-security-release-breakdown.html
●	WP < 6.0.2 - SQLi via Link API	5.1.14	N/A	5.8	https://wordpress.org/news/2022/08/wordpress-6-0-2-security-and-maintenance-release/
●	WordPress < 5.9.2 - Prototype Pollution in jQuery	5.1.13	N/A	5.6	https://wordpress.org/news/2022/03/wordpress-5-9-2-security-maintenance-release/
●	WordPress <= 5.2.3 - Stored XSS in Customizer	5.1.3	2019-17674	5.4	https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/ https://blog.wpscan.com/wordpress/security/release/2019/10/15/wordpress-524-security-release-breakdown.html
●	WordPress < 5.4.2 - Authenticated XSS in Block Editor	5.1.6	2020-4046	5.4	https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/ https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-rpwf-hrh2-39jf https://pentest.co.uk/labs/research/subtle-stored-xss-wordpress-core/
●	WordPress < 5.8.3 - Author+ Stored XSS via Post Slugs	5.1.12	2022-21662	5.4	https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-699q-3hj9-889w https://hackerone.com/reports/425342 https://blog.sonarsource.com/wordpress-stored-xss-vulnerability
●	WP <= 6.1.1 - Unauthenticated Blind SSRF via DNS Rebinding	N/A	2022-3590	5.4	https://blog.sonarsource.com/wordpress-core-unauthenticated-blind-ssrf/
●	WordPress <= 5.2.3 - Unauthenticated View Private/Draft Posts	5.1.3	2019-17671	5.3	https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/ https://blog.wpscan.com/wordpress/security/release/2019/10/15/wordpress-524-security-release-breakdown.html https://github.com/WordPress/WordPress/commit/f82ed753cf00329a5e41f2cb6dc521085136f308 https://0day.work/proof-of-concept-for-wordpress-5-2-3-viewing-unauthenticated-posts/

●	WP < 6.0.3 - Stored XSS via wp-mail.php	5.1.15	N/A	4.8	https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/ https://github.com/WordPress/wordpress-develop/commit/abf236fdaf94455e7bc6e30980cf70401003e283
●	WP < 6.0.2 - Reflected Cross-Site Scripting	5.1.14	N/A	4.7	https://wordpress.org/news/2022/08/wordpress-6-0-2-security-and-maintenance-release/
●	WP < 6.0.3 - Reflected XSS via SQLi in Media Library	5.1.15	N/A	4.7	https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/ https://github.com/WordPress/wordpress-develop/commit/8836d4682264e8030067e07f2f953a0f66cb76cc
●	WordPress <= 5.3 - Authenticated Stored XSS via Block Editor Content	5.1.4	2019-16781	4.6	https://wordpress.org/news/2019/12/wordpress-5-3-1-security-and-maintenance-release/ https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-pg4x-64rh-3c9v
●	WordPress < 5.4.1 - Authenticated Cross-Site Scripting (XSS) in File Uploads	5.1.5	2020-11026	4.6	https://wordpress.org/news/2020/04/wordpress-5-4-1/ https://core.trac.wordpress.org/changeset/47638/ https://www.wordfence.com/blog/2020/04/unpacking-the-7-vulnerabilities-fixed-in-todays-wordpress-5-4-1-security-update/ https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-3gw2-4656-pfr2 https://hackerone.com/reports/179695
●	WP < 6.0.3 - Stored XSS via Comment Editing	5.1.15	N/A	4.4	https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/ https://github.com/WordPress/wordpress-develop/commit/89c8f7919460c31c0f259453b4ffb63fde9fa955
●	WordPress < 5.4.2 - Disclosure of Password-Protected Page/Post Comments	5.1.6	2020-25286	4.3	https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/ https://github.com/WordPress/WordPress/commit/c075eec24f2f3214ab0d0fb0120a23082e6b1122
●	WordPress 4.7-5.7 - Authenticated Password Protected Pages Exposure	5.1.9	2021-29450	4.3	https://wordpress.org/news/2021/04/wordpress-5-7-1-security-and-maintenance-release/ https://blog.wpscan.com/2021/04/15/wordpress-571-security-vulnerability-release.html https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-pmmh-2f36-wvhq https://core.trac.wordpress.org/changeset/50717/
●	WP < 6.0.3 - Open Redirect via wp_nonce_ays	5.1.15	N/A	4.3	https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/ https://github.com/WordPress/wordpress-develop/commit/506eee125953deb658307bb3005417cb83f32095
●	WP < 6.0.3 - Data Exposure via REST Terms/Tags Endpoint	5.1.15	N/A	4.3	https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/ https://github.com/WordPress/wordpress-develop/commit/ebaac57a9ac0174485c65de3d32ea56de2330d8e
●	WordPress < 5.4.1 - Cross-Site Scripting (XSS) in wp-object-cache	5.1.5	2020-11029	4.2	https://wordpress.org/news/2020/04/wordpress-5-4-1/ https://core.trac.wordpress.org/changeset/47637/ https://www.wordfence.com/blog/2020/04/unpacking-the-7-vulnerabilities-fixed-in-todays-wordpress-5-4-1-security-update/ https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-568w-8m88-8g2c
●	WP < 6.0.3 - SQLi in WP_Date_Query	5.1.15	N/A	4	https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/ https://github.com/WordPress/wordpress-develop/commit/d815d2e8b2a7c2be6694b49276ba3eee5166c21f

●	WordPress <= 5.3 - Authenticated Stored XSS via Crafted Links	5.1.4	2019-20042	3.8	https://wordpress.org/news/2019/12/wordpress-5-3-1-security-and-maintenance-release/ https://hackerone.com/reports/509930 https://github.com/WordPress/wordpress-develop/commit/1f7f3f1f59567e2504f0fbebd51ccf004b3ccb1d https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-xvg2-m2f4-83m7
●	WordPress < 5.4.2 - Authenticated Stored XSS via Theme Upload	5.1.6	2020-4049	3.8	https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/ https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-87h4-phjv-rm6p https://hackerone.com/reports/406289
●	WordPress < 5.4.1 - Unauthenticated Users View Private Posts	5.1.5	2020-11028	3.7	https://wordpress.org/news/2020/04/wordpress-5-4-1/ https://core.trac.wordpress.org/changeset/47635/ https://www.wordfence.com/blog/2020/04/unpacking-the-7-vulnerabilities-fixed-in-todays-wordpress-5-4-1-security-update/ https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-xhx9-759f-6p2w
●	WordPress < 5.4.1 - Authenticated Cross-Site Scripting (XSS) in Customizer	5.1.5	2020-11025	3.7	https://wordpress.org/news/2020/04/wordpress-5-4-1/ https://core.trac.wordpress.org/changeset/47633/ https://www.wordfence.com/blog/2020/04/unpacking-the-7-vulnerabilities-fixed-in-todays-wordpress-5-4-1-security-update/ https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-4mhg-j6fx-5g3c
●	WP < 6.0.3 - Content from Multipart Emails Leaked	5.1.15	N/A	3.7	https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/ https://github.com/WordPress/wordpress-develop/commit/3765886b4903b319764490d4ad5905bc5c310ef8
●	WordPress < 5.4.2 - Open Redirection	5.1.6	2020-4048	3.5	https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/ https://github.com/WordPress/WordPress/commit/10e2a50c523cf0b9785555a688d7d36a40fbeccf https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-q6pw-gvf4-5fj5
●	WP < 6.0.3 - Stored XSS via the Customizer	5.1.15	N/A	3.4	https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/ https://github.com/WordPress/wordpress-develop/commit/2ca28e49fc489a9bb3c9c9c0d8907a033fe056ef
●	WP < 6.0.3 - Multiple Stored XSS via Gutenberg	5.1.15	N/A	3.4	https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/ https://github.com/WordPress/gutenberg/pull/45045/files
●	WordPress < 5.8.3 - Super Admin Object Injection in Multisites	5.1.12	2022-21663	3.3	https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-jmmq-m8p8-332h https://hackerone.com/reports/541469
●	WordPress < 5.4.1 - Password Reset Tokens Failed to Be Properly Invalidated	5.1.5	2020-11027	3.1	https://wordpress.org/news/2020/04/wordpress-5-4-1/ https://core.trac.wordpress.org/changeset/47634/ https://www.wordfence.com/blog/2020/04/unpacking-the-7-vulnerabilities-fixed-in-todays-wordpress-5-4-1-security-update/ https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-ww7v-jg8c-q6jw
●	WordPress <= 5.2.3 - Hardening Bypass	5.1.3	N/A	3.1	https://blog.ripstech.com/2020/wordpress-hardening-bypass/ https://hackerone.com/reports/436928 https://wordpress.org/news/2019/11/wordpress-5-2-4-update/
●	WP < 6.0.3 - Email Address Disclosure via wp-mail.php	5.1.15	N/A	3.1	https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/ https://github.com/WordPress/wordpress-develop/commit/5fcdee1b4d72f1150b7b762ef5fb39ab288c8d44

●	WP < 6.0.3 - CSRF in wp-trackback.php	5.1.15	N/A	3.1	https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/ https://github.com/WordPress/wordpress-develop/commit/a4f9ca17fae0b7d97ff807a3c234cf219810fae0
●	WP < 6.0.3 - Stored XSS via RSS Widget	5.1.15	N/A	3	https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/ https://github.com/WordPress/wordpress-develop/commit/929cf3cb9580636f1ae3fe944b8faf8cca420492
●	WP < 6.0.2 - Authenticated Stored Cross-Site Scripting	5.1.14	N/A	2.6	https://wordpress.org/news/2022/08/wordpress-6-0-2-security-and-maintenance-release/
●	WordPress <= 5.3 - Authenticated Improper Access Controls in REST API	5.1.4	2019-20043	0	https://wordpress.org/news/2019/12/wordpress-5-3-1-security-and-maintenance-release/ https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-g7rg-hchx-c2gw

Details

Risk description:
Depending on the specific details of the vulnerabilities, an attacker could exploit them to affect the confidentiality 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.

Classification:
CWE : CWE-1026
OWASP Top 10 - 2013 : A9 - Using Components with Known Vulnerabilities
OWASP Top 10 - 2017 : A9 - Using Components with Known Vulnerabilities

Vulnerable WordPress theme detected

Theme information

Theme name: ripple
Theme version: 1.2.0
Location: http://testing1.pentest-tools.com:9000/wp-content/themes/ripple/
Latest version: 1.2.1
Last updated: 2022-02-26T00:00:00.000Z
Outdated: True
Readme URL: http://testing1.pentest-tools.com:9000/wp-content/themes/ripple/readme.txt
Style URL: http://testing1.pentest-tools.com:9000/wp-content/themes/ripple/style.css
Style name: Ripple
Style uri: https://accesspressthemes.com/wordpress-themes/ripple
Description: Ripple is a versatile one page WordPress theme for creating beautiful One Page websites. This theme comes with powerful customizer based options allowing you to build the wonderful websites in no time. Ripple is flexible, lightweight and it comes with a clean and flat design. It is not only limited to one page websites, You may also build website for any type of niche - Corporate, Agency, Portfolio etc to name some. The theme contains a beautiful filter based portfolio sections, Attractive call to action and many more. You may find the demo for Ripple theme here https://demo.accesspressthemes.com/ripple/.
Author: AccessPress Themes
Author uri: http://accesspressthemes.com
License: GNU General Public License, version 3 (GPLv3)
License uri: http://www.gnu.org/licenses/gpl-3.0.txt
Tags: right-sidebar, featured-images, full-width-template, rtl-language-support, threaded-comments, translation-ready, two-columns, custom-logo, footer-widgets, theme-options, portfolio, blog
Text domain: ripple
Found by: Known Locations (Aggressive Detection)

Risk level	Vulnerability title	Fixed in	CVE	CVSS	Reference URLs
●	Backdoored Plugins & Themes from AccessPress Themes	1.2.1	2021-24867	10	https://jetpack.com/2022/01/18/backdoor-found-in-themes-and-plugins-from-accesspress-themes/

Details

Risk description:
An attacker could exploit these vulnerabilities to affect the confidentiality and the integrity of the application's data or to affect the availability of the application.

Recommendation:
Update the affected theme to the latest version.

Classification:
CWE : CWE-1026
OWASP Top 10 - 2013 : A9 - Using Components with Known Vulnerabilities
OWASP Top 10 - 2017 : A9 - Using Components with Known Vulnerabilities

Vulnerable WordPress theme detected

Theme information

Theme name: twentyfifteen
Theme version: 1.1
Location: http://testing1.pentest-tools.com:9000/wp-content/themes/twentyfifteen/
Latest version: 3.3
Last updated: 2022-11-02T00:00:00.000Z
Outdated: True
Readme URL: http://testing1.pentest-tools.com:9000/wp-content/themes/twentyfifteen/readme.txt
Style URL: http://testing1.pentest-tools.com:9000/wp-content/themes/twentyfifteen/style.css
Style name: Twenty Fifteen
Style uri: https://wordpress.org/themes/twentyfifteen/
Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's simple, straightforward typography is readable on a wide variety of screen sizes, and suitable for multiple languages. We designed it using a mobile-first approach, meaning your content takes center-stage, regardless of whether your visitors arrive by smartphone, tablet, laptop, or desktop computer.
Author: the WordPress team
Author uri: https://wordpress.org/
License: GNU General Public License v2 or later
License uri: http://www.gnu.org/licenses/gpl-2.0.html
Tags: black, blue, gray, pink, purple, white, yellow, dark, light, two-columns, left-sidebar, fixed-layout, responsive-layout, accessibility-ready, custom-background, custom-colors, custom-header, custom-menu, editor-style, featured-images, microformats, post-formats, rtl-language-support, sticky-post, threaded-comments, translation-ready
Text domain: twentyfifteen
Found by: Known Locations (Aggressive Detection)

Risk level	Vulnerability title	Fixed in	CVE	CVSS	Reference URLs
●	Twenty Fifteen Theme <= 1.1 - DOM Cross-Site Scripting (XSS)	1.2	2015-3429	N/A	https://blog.sucuri.net/2015/05/jetpack-and-twentyfifteen-vulnerable-to-dom-based-xss-millions-of-wordpress-websites-affected-millions-of-wordpress-websites-affected.html https://packetstormsecurity.com/files/131802/ https://seclists.org/fulldisclosure/2015/May/41

Details

Risk description:
An attacker could exploit these vulnerabilities to affect the confidentiality and the integrity of the application's data or to affect the availability of the application.

Recommendation:
Update the affected theme to the latest version.

Classification:
CWE : CWE-1026
OWASP Top 10 - 2013 : A9 - Using Components with Known Vulnerabilities
OWASP Top 10 - 2017 : A9 - Using Components with Known Vulnerabilities

Vulnerable WordPress plugin detected

Plugin information

Plugin name: akismet
Plugin version: 3.0.0
Location: http://testing1.pentest-tools.com:9000/wp-content/plugins/akismet/
Latest version: 5.1
Last updated: 2023-03-20T19:29:00.000Z
Outdated: True
Readme URL: http://testing1.pentest-tools.com:9000/wp-content/plugins/akismet/readme.txt
Found by: Known Locations (Aggressive Detection)
Other evidence:
http://testing1.pentest-tools.com:9000/wp-content/plugins/akismet/readme.txt

Risk level	Vulnerability title	Fixed in	CVE	CVSS	Reference URLs
●	Akismet 2.5.0-3.1.4 - Unauthenticated Stored Cross-Site Scripting (XSS)	3.1.5	2015-9357	6.1	http://blog.akismet.com/2015/10/13/akismet-3-1-5-wordpress/ https://blog.sucuri.net/2015/10/security-advisory-stored-xss-in-akismet-wordpress-plugin.html

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 confidentiality 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.
If this plugin is not used, it may have been previously installed and still resides on the web server. We then recommend removing it from the path provided.

Classification:
CWE : CWE-1026
OWASP Top 10 - 2013 : A9 - Using Components with Known Vulnerabilities
OWASP Top 10 - 2017 : A9 - Using Components with Known Vulnerabilities

Vulnerable WordPress plugin detected

Plugin information

Plugin name: mailchimp-for-wp
Plugin version: 4.8.6
Location: http://testing1.pentest-tools.com:9000/wp-content/plugins/mailchimp-for-wp/
Latest version: 4.9.2
Last updated: 2023-03-21T08:19:00.000Z
Outdated: True
Readme URL: http://testing1.pentest-tools.com:9000/wp-content/plugins/mailchimp-for-wp/readme.txt
Found by: Known Locations (Aggressive Detection)
Other evidence:
http://testing1.pentest-tools.com:9000/wp-content/plugins/mailchimp-for-wp/readme.txt

Risk level	Vulnerability title	Fixed in	CVE	CVSS	Reference URLs
●	MC4WP < 4.8.7 - Admin+ Stored Cross-Site Scripting	4.8.7	N/A	3.4	https://plugins.trac.wordpress.org/changeset/2687297
●	MC4WP < 4.8.7 - Admin+ Stored Cross-Site Scripting	4.8.7	2021-36833	3.4	https://www.hackpertise.com/cve/30-cve-2021-36833/

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 confidentiality 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.
If this plugin is not used, it may have been previously installed and still resides on the web server. We then recommend removing it from the path provided.

Classification:
CWE : CWE-1026
OWASP Top 10 - 2013 : A9 - Using Components with Known Vulnerabilities
OWASP Top 10 - 2017 : A9 - Using Components with Known Vulnerabilities

Users discovered during enumeration

Username	Interesting Entries
wordpress_admin	http://testing1.pentest-tools.com:9000/wp-json/wp/v2/users/?per_page=100&page=1

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.

Furthermore, reconfigure WordPress to deny user enumeration.

References:
https://perishablepress.com/stop-user-enumeration-wordpress/

Classification:
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Interesting headers found

URL	Found by	Interesting Entries
http://testing1.pentest-tools.com:9000/	Headers (Passive Detection)	Server: Apache/2.4.25 (Debian) X-Powered-By: PHP/7.2.18

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 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Found robots.txt file

URL	Found by	Interesting Entries
http://testing1.pentest-tools.com:9000/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 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Found xmlrpc file

URL	Found by	Method	Parameters	Replay request
http://testing1.pentest-tools.com:9000/xmlrpc.php	Direct Access (Aggressive Detection)	POST	Body: <?xml version="1.0"?> <methodCall> <methodName> demo.sayHello</methodName> <params></params> </methodCall>	🚀

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.

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

References:
http://codex.wordpress.org/XML-RPC_Pingback_API

Classification:
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Found default Readme file

URL	Found by
http://testing1.pentest-tools.com:9000/readme.html	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 help mount further attacks.

Recommendation:
Remove the Readme file.

Classification:
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Found wp-cron file

URL	Found by
http://testing1.pentest-tools.com:9000/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 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Scan finished successfully

Main theme twentyseventeen 2.1 has no known vulnerabilities

No config backups found

No database exports found

No timthumbs found

Scan coverage information

List of tests performed (16/16)

- ✓ Scanning with WPScan... (this may take a while)
- ✓ Searching for WordPress vulnerabilities...
- ✓ Searching for main theme vulnerabilities...
- ✓ Searching vulnerabilities for theme: ripple
- ✓ Searching vulnerabilities for theme: twentyfifteen
- ✓ Searching vulnerabilities for plugin: akismet
- ✓ Searching vulnerabilities for plugin: mailchimp-for-wp
- ✓ Attempting user enumeration...
- ✓ Searching for config backups...
- ✓ Searching for database exports...
- ✓ Searching for timthumbs...
- ✓ Checking for valuable information in HTTP headers...
- ✓ Checking for the robots.txt file...
- ✓ Checking whether XML-RPC is enabled...
- ✓ Checking for the presence of the WordPress readme file...
- ✓ Checking whether wp-cron is enabled...

Scan parameters

Target:	http://testing1.pentest-tools.com:9000
Detection mode:	Aggressive
Enumerate users:	True
Enumerate vulnerable plugins:	True
Enumerate vulnerable themes:	True
Enumerate config backups:	True
Enumerate database exports:	True
Enumerate TimThumbs:	True