WordPress Vulnerability Scan Report

==========
Scanned Website: https://example.com Scan Date and Time: 2025-07-31 08:48:12 Tool Version: 1.0.0
==========

Vulnerability Summary

High Severity: 0 Medium Severity: 0 Low Severity: 0

Vulnerability Name: Remote Code Execution (RCE)

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Ability to execute arbitrary code remotely on the server.
- Remediation: Regularly update all plugins, themes, and WordPress core. Use a Web Application Firewall (WAF).

Vulnerability Name: SQL Injection (SQLi)

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Ability to inject malicious SQL queries into the database.
- Remediation: Use Prepared Statements or ORMs. Validate all user inputs.

Vulnerability Name: Authentication Bypass

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Bypassing authentication mechanisms for unauthorized access.
- Remediation: Implement strong authentication, update WordPress and plugins, use Two-Factor Authentication (2FA).

Vulnerability Name: Privilege Escalation

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Ability for low-privileged users to gain higher privileges.

- Remediation: Apply the principle of least privilege, update all components, regularly review user permissions.

Vulnerability Name: File Upload Vulnerability

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Ability to upload malicious files (e.g., web shells) to the server.
- Remediation: Strictly validate file type, size, and content. Store uploaded files outside the public web root. Rename uploaded files.

Vulnerability Name: Local File Inclusion (LFI)

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Ability to include local files from the server.
- Remediation: Avoid using user input directly in file paths. Use a whitelist for allowed files. Disable `allow_url_include` in PHP.

Vulnerability Name: Directory Traversal

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Ability to access files and directories outside the intended directory.
- Remediation: Validate user input. Use absolute paths or sanitize input to remove '..' sequences.

Vulnerability Name: Insecure Deserialization

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Ability to exploit serialized data to execute code.
- Remediation: Avoid deserializing untrusted data. Use secure data formats like JSON. Validate data integrity before deserialization.

Vulnerability Name: Arbitrary File Deletion

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Ability to delete any file on the server.
- Remediation: Apply strict access controls to file deletion functions. Validate user permissions and file path before deletion.

Vulnerability Name: Arbitrary File Read

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Ability to read any file on the server.
- Remediation: Apply strict access controls to file reading functions. Validate user permissions and file path before reading.

Vulnerability Name: Arbitrary File Write

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Ability to write any file on the server.
- Remediation: Apply strict access controls to file writing functions. Validate user permissions and file path before writing.

Vulnerability Name: Server-Side Request Forgery (SSRF)

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Ability to force the server to make HTTP requests to internal or external locations.
- Remediation: Validate user-supplied URLs. Use a whitelist for allowed domains. Disable redirects.

Vulnerability Name: XML External Entity (XXE)

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Ability to exploit XML parsing to read local files or perform SSRF attacks.
- Remediation: Disable support for external entities in XML parsers. Update libraries.

Vulnerability Name: Command Injection

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Ability to execute operating system commands on the server.
- Remediation: Avoid using user input directly in system commands. Use safe APIs. Validate input.

Vulnerability Name: Unauthenticated Admin Access

- Scan Status: ✅ Not Detected

- Severity: High
- Description: Access to the admin panel without authentication.
- Remediation: Secure the admin panel with a strong password and 2FA. Restrict access to /wp-admin from trusted IP addresses.

Vulnerability Name: Shell Upload via Theme/Plugin Editor

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Ability to upload malicious shells via the theme/plugin editor.
- Remediation: Disable the theme and plugin editor from the WordPress dashboard (via `define('DISALLOW_FILE_EDIT', true);` in wp-config.php).

Vulnerability Name: Cross-Site Scripting (XSS)

- Scan Status: ✅ Not Detected
- Severity: Medium
- Description: Ability to inject malicious JavaScript into website pages.
- Remediation: Sanitize all user inputs, use Content Security Policy (CSP), encode outputs.

Vulnerability Name: Cross-Site Request Forgery (CSRF)

- Scan Status: ✅ Not Detected
- Severity: Medium
- Description: Ability to perform unwanted actions on behalf of an authenticated user.
- Remediation: Use CSRF tokens, validate HTTP Referer header, use SameSite cookies.

Vulnerability Name: Open Redirect

- Scan Status: ✅ Not Detected
- Severity: Medium
- Description: Ability to redirect users to malicious websites.
- Remediation: Validate input URLs, use a whitelist for allowed domains.

Vulnerability Name: Information Disclosure

- Scan Status: ✅ Not Detected
- Severity: Medium
- Description: Disclosure of sensitive information such as version numbers or file paths.

- Remediation: Hide version numbers, disable error display in production, secure configuration files.

Vulnerability Name: REST API Unauthorized Access

- Scan Status: ✅ Not Detected
- Severity: Medium
- Description: Unauthorized access to the WordPress REST API.
- Remediation: Restrict REST API access, use proper authentication, disable unused endpoints.

Vulnerability Name: Insecure Direct Object Reference (IDOR)

- Scan Status: ✅ Not Detected
- Severity: Medium
- Description: Access to unauthorized objects or data by changing object identifiers.
- Remediation: Apply strict access controls, validate user permissions before accessing objects.

Vulnerability Name: Clickjacking

- Scan Status: ✅ Detected
- Severity: Medium
- Description: Ability to trick users into clicking on hidden or misleading elements.
- Remediation: Use X-Frame-Options header or Content Security Policy (CSP) frame-ancestors directive.

Vulnerability Name: Open Port / Misconfigured Services

- Scan Status: ✅ Not Detected
- Severity: Medium
- Description: Presence of open ports or misconfigured services.
- Remediation: Close unused ports, secure exposed services, use a firewall.

Vulnerability Name: Exposed Debug Logs

- Scan Status: ✅ Not Detected
- Severity: Medium
- Description: Exposure of debug log files that may contain sensitive information.
- Remediation: Disable debug logging in production, protect log files from public access.

Vulnerability Name: Directory Indexing

- Scan Status: ✅ Not Detected
- Severity: Medium
- Description: Ability to view directory contents via the browser.
- Remediation: Disable directory listing in server settings, add empty index.html files to sensitive directories.

Vulnerability Name: Version Disclosure

- Scan Status: ✅ Not Detected
- Severity: Medium
- Description: Disclosure of WordPress, plugin, or theme versions.
- Remediation: Hide version numbers from HTML source, use plugins to hide version information.

Vulnerability Name: Reflected File Download

- Scan Status: ✅ Not Detected
- Severity: Medium
- Description: Ability to trick users into downloading malicious files.
- Remediation: Validate file names and content, use appropriate Content-Disposition headers.

Vulnerability Name: Content Spoofing

- Scan Status: ✅ Not Detected
- Severity: Medium
- Description: Ability to forge page content to deceive users.
- Remediation: Sanitize user input, use Content Security Policy (CSP).

Vulnerability Name: Insecure File Permissions

- Scan Status: ✅ Not Detected
- Severity: Medium
- Description: Insecure file permissions that may allow unauthorized access.
- Remediation: Apply appropriate file permissions (644 for files, 755 for directories), protect wp-config.php.

Vulnerability Name: Theme/Plugin Path Disclosure

- Scan Status: ✅ Not Detected
- Severity: Medium

- Description: Disclosure of theme and plugin paths, which helps attackers target them.
- Remediation: Hide theme and plugin paths, use plugins to hide this information.

Vulnerability Name: Exposed XML-RPC

- Scan Status: ✅ Not Detected
- Severity: Medium
- Description: Exposure of XML-RPC endpoint allowing brute force and DDoS attacks.
- Remediation: Disable XML-RPC if not used, or restrict access to it.

Vulnerability Name: Weak wp-config.php permissions

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Weak permissions on wp-config.php file that may allow it to be read.
- Remediation: Apply 600 or 644 permissions to wp-config.php, move it outside the public folder.

Vulnerability Name: No HTTP Security Headers

- Scan Status: ✅ Detected
- Severity: Medium
- Description: Absence of HTTP security headers like CSP, X-Frame-Options, etc.
- Remediation: Add HTTP security headers: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, etc.

Vulnerability Name: Admin Panel Exposed

- Scan Status: ✅ Not Detected
- Severity: Medium
- Description: Admin panel exposed without additional protection.
- Remediation: Restrict access to /wp-admin from trusted IP addresses, use .htaccess or a firewall.

Vulnerability Name: Default Usernames

- Scan Status: ✅ Not Detected
- Severity: Medium
- Description: Use of default usernames like 'admin' or 'administrator'.
- Remediation: Change default usernames, use strong and unpredictable usernames.

Vulnerability Name: Weak Passwords (Brute-force vulnerability)

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Use of weak passwords susceptible to brute-force attacks.
- Remediation: Use strong passwords, enforce password policies, use plugins to prevent brute force.

Vulnerability Name: No 2FA

- Scan Status: ✅ Not Detected
- Severity: Medium
- Description: Absence of Two-Factor Authentication (2FA).
- Remediation: Implement 2FA for all users, especially administrators.

Vulnerability Name: No CAPTCHA on Login

- Scan Status: ✅ Not Detected
- Severity: Medium
- Description: Absence of CAPTCHA on the login page, facilitating brute-force attacks.
- Remediation: Add CAPTCHA to the login page, use plugins like reCAPTCHA.

Vulnerability Name: Auto Indexing Enabled

- Scan Status: ✅ Not Detected
- Severity: Medium
- Description: Automatic directory indexing enabled, exposing their contents.
- Remediation: Disable directory listing in server settings, add empty index.html files.

Vulnerability Name: Backup Files Exposed

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Exposure of backup files (.zip, .sql, .bak) to the public.
- Remediation: Protect backup files, store them outside the public folder, use .htaccess to prevent access.

Vulnerability Name: WP-Cron Abuse

- Scan Status: ✅ Not Detected
- Severity: Low
- Description: Ability to exploit WP-Cron for DDoS attacks or resource exhaustion.
- Remediation: Disable public WP-Cron and use a real cron job, or restrict access to wp-cron.php.

Vulnerability Name: File Editor Enabled

- Scan Status: ✅ Not Detected
- Severity: High
- Description: File editor enabled in the dashboard, allowing modification of PHP files.
- Remediation: Disable the file editor by adding `define('DISALLOW_FILE_EDIT', true);` in wp-config.php.

Vulnerability Name: Nulled Themes/Plugins (with Backdoors)

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Using pirated themes or plugins that may contain backdoors.
- Remediation: Use only original themes and plugins from trusted sources, scan files for malicious code.

Vulnerability Name: Insecure Update Mechanism

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Insecure update mechanism for plugins or themes.
- Remediation: Use HTTPS for all updates, verify digital signatures, regularly update WordPress and plugins.

Vulnerability Name: Insecure AJAX Actions

- Scan Status: ✅ Not Detected
- Severity: Medium
- Description: Unprotected AJAX actions allowing unauthorized operations.
- Remediation: Apply nonce verification to all AJAX actions, validate user permissions.

Vulnerability Name: Missing Nonce Verification

- Scan Status: ✅ Not Detected
- Severity: Medium
- Description: Absence of nonce verification allowing CSRF attacks.
- Remediation: Apply nonce verification to all sensitive forms and actions.

Vulnerability Name: Plugin with Publicly Known Exploits

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Using plugins with known public security vulnerabilities.
- Remediation: Update all plugins to the latest versions, remove unused plugins, monitor security updates.

Vulnerability Name: Demo Importer Exploits

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Exploiting demo importer tools to upload malicious files.
- Remediation: Disable or remove demo importer tools after setup, restrict access to them.

Vulnerability Name: Malicious Shortcodes

- Scan Status: ✅ Not Detected
- Severity: Medium
- Description: Presence of malicious shortcodes that can execute unwanted code.
- Remediation: Review all used shortcodes, remove untrusted plugins, scan content for suspicious shortcodes.

Vulnerability Name: Insecure Widget Code

- Scan Status: ✅ Not Detected
- Severity: Medium
- Description: Insecure code in widgets that can lead to security vulnerabilities.
- Remediation: Review all widget code, avoid using widgets from untrusted sources.

Vulnerability Name: Theme/Plugin Options Injection

- Scan Status: ✅ Not Detected
- Severity: High

- Description: Ability to inject malicious options into theme or plugin settings.
- Remediation: Validate all theme and plugin options, apply strict access controls.

Vulnerability Name: No Access Control on Custom Endpoints

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Lack of access controls on custom endpoints.
- Remediation: Apply strict access controls to all custom endpoints, validate user permissions.

Vulnerability Name: Arbitrary Options Update (update_option Vulnerability)

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Ability to arbitrarily update WordPress options.
- Remediation: Apply strict access controls to `update_option` functions, validate user permissions.

Vulnerability Name: Arbitrary User Creation

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Ability to arbitrarily create new users.
- Remediation: Apply strict access controls to user creation functions, disable public registration if not required.

Vulnerability Name: Theme Function Injection via functions.php

- Scan Status: ✅ Not Detected
- Severity: High
- Description: Ability to inject malicious code into the theme's functions.php file.
- Remediation: Protect functions.php from modification, review all changes to theme files.

--- End of Report --- Signature: O-WPScan Tool Developer: Eng. Omar Hany Shalaby