WordPress Vulnerability Scanner - WPScan Report

Summary

Overall risk level: Medium

Risk ratings:
- High: 0
- Medium: 4
- Low: 4
- Info: 3

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**
  - 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**

<table>
<thead>
<tr>
<th>Vulnerability title</th>
<th>Fixed in</th>
<th>CVE</th>
<th>CVSS</th>
<th>Reference URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><a href="https://github.com/WordPress/WordPress/commit/80436385602d405d09a38a21f5a65d9a3c18216">https://github.com/WordPress/WordPress/commit/80436385602d405d09a38a21f5a65d9a3c18216</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><a href="https://github.com/WordPress/WordPress/commit/80436385602d405d09a38a21f5a65d9a3c18216">https://github.com/WordPress/WordPress/commit/80436385602d405d09a38a21f5a65d9a3c18216</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><a href="https://github.com/WordPress/WordPress/commit/14be2e166f0d0a04b4f71070e01dc8503edc8e">https://github.com/WordPress/WordPress/commit/14be2e166f0d0a04b4f71070e01dc8503edc8e</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><a href="http://blog.dewhurtssecurity.com/2017/05/04/exploitbox-wordpress-security-advisories.html">http://blog.dewhurtssecurity.com/2017/05/04/exploitbox-wordpress-security-advisories.html</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><a href="https://core.trac.wordpress.org/ticket/25239">https://core.trac.wordpress.org/ticket/25239</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><a href="https://github.com/WordPress/WordPress/commit/369c0b1e71cfe4ab5e0023992964fct1198d850">https://github.com/WordPress/WordPress/commit/369c0b1e71cfe4ab5e0023992964fct1198d850</a></td>
</tr>
</tbody>
</table>
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 affected plugin to the latest version.

Vulnerability title

Tribulant Newsletters < 4.6.4.2 Allow Multiple Vul

4.6.5

N/A

N/A


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.

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
No additional themes found

Scan finished successfully

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 for additional vulnerabilities for plugin newsletters-lite
- Attempting user enumeration...

Scan parameters

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